



CenterStone Security

Version 1.0.5
February, 2007
Company Confidential

| | |
|--|-----------|
| CenterStone Security Data Sheet | 4 |
| Internet Access | 5 |
| CenterStone Network Configuration | 5 |
| Application Security | 6 |
| Usernames and Passwords | 6 |
| The Client Applet..... | 8 |
| Functional & Data Access Control Security..... | 9 |
| Data Imports..... | 11 |
| Hosting Environment..... | 12 |
| Managed Hosting Center (Data Center)..... | 14 |
| CenterStone Hosted Architecture | 15 |
| SAS 70 Compliance..... | 16 |
| Network Security Architecture..... | 17 |
| Firewalls..... | 17 |
| Encryption | 19 |
| OS and Security Patching & Hardening..... | 20 |
| Active Network Monitoring and Intrusion Detection | 21 |
| External Audits | 22 |
| Predictive Systems | 22 |
| Network Penetration Tests..... | 24 |
| Application Updates..... | 25 |
| Backup and Disaster Recovery | 26 |
| Data Storage and Backup Procedures | 26 |
| <i>Backup Frequencies</i> | 26 |
| <i>Standard Operating Procedures</i> | 28 |
| Secure Redundancy Using Multiple Hosting Providers | 29 |
| <i>Disaster Definition</i> | 29 |
| Catastrophic Condition (Level 2)..... | 29 |
| Minor Condition Recovery | 31 |
| Major Condition Recovery | 32 |
| Catastrophic Condition Recovery (Phase I)..... | 33 |

Catastrophic Condition Recovery (Phase II) 34
Catastrophic Condition Recovery (Phase II) Recovery Flow 35
Security Guidelines36
Facility Security Standards.....37
Glossary & Index of Terms.....38
Confidentiality Notice.....40

CenterStone Security Data Sheet

Manhattan CenterStone is the leading provider of internet-based Workplace Resource Management solutions. Its flagship product, CenterStone, is an integrated collaborative platform used by workplace managers, planners, and executives to consolidate workplace data into a single web-based solution for decision making, operational planning, and strategic analysis.

CenterStone integrates multiple product modules, software products, and internal applications that manage independent areas of the workplace: real estate, facilities, IT, security, HR, space plans, and capital projects, to create a single corporate workplace portal. This consolidated view enables collaboration across departments, projects, people and partners to create a cost-efficient, productive workplace.

Network security is all about protecting system devices and the data they store and forward. Since CenterStone is a web-based solution for Workplace Resource Management, Manhattan CenterStone treats security issues as a top priority for its customers.

The Internet is the entry point to CenterStone. Although each server is protected by its own OS gatekeeper, it is important to keep the servers from being deluged by attacks coming from the network layer. Of equal importance is not allowing unauthorized entities to replace or reconfigure the network gatekeeper, or otherwise exploit network device vulnerabilities. The CenterStone total security solution enhances gatekeeping that controls external access to the servers in your application environment.

At Manhattan CenterStone we realize that the availability of workplace information managed in the CenterStone Workplace Resource Management platform at our hosting provider is vital to the day-to-day operations of our customers. As such, we have put into place state of the art infrastructure, procedures and best practices to ensure that our customers' information is secure and recoverable.

Internet Access

Manhattan CenterStone's CenterStone application is web-based, and requires only that its customers have

- Internet access
- TCP/IP ports 443 (https) or 80 (http) enabled on the client firewall(s) and router(s). CenterStone does not use any other ports, and our customer's site can be locked down to requiring 128-bit SSL. The front-end firewall is locked down to only allow access through ports 443 and 80.

CenterStone Network Configuration

Manhattan CenterStone has designed the CenterStone application as a hosted Internet application. The hosted database server operates Microsoft SQL Server 2000, the hosted web server operates Microsoft Internet Information Services, and the hosted application server operates BEA WebLogic.

On client personal computers, the CenterStone application supports Netscape Navigator (4.x and higher) or Microsoft Internet Explorer (5.x and higher). The client also utilizes Sun Microsystem's Java plug-in (1.4.2 or higher), which is automatically detected and downloaded to the user's system if required.

Manhattan CenterStone utilizes a *tiered* firewall approach, with the Web server behind the first, or front-end, firewall, and the Database and Application servers behind the second, or inner, firewall. All traffic between the Web server and the Application server is through this inner firewall. CenterStone uses the WebLogic IIS plug-in to route traffic between the Web server and the Application server, so users coming through the Web server never directly access the Application or Database server.

As an additional security measure, the Application and Database servers use private non-routable IP addresses. Static routes are individually added to the Application and Database services to permit access.

Application Security

Manhattan CenterStone has designed CenterStone from the ground up to support high-availability and industry-leading security. In addition to secure communications over the Internet and the hosting partnership with CSC, CenterStone includes an application-level security model.

All customers have unique and separate databases at the hosting data center, which ensures complete segregation and integrity of the customer's data.

A flexible, rules-based security architecture is built into CenterStone's core. This architecture limits the information users can see and what functionality within the application that they can use. Customers can decide who sees what, including Building information, Leases, Project details, and who is moving into the new corner office. Also, Administrators can determine the level of data access that a user has – for example, restrict the user to only being able to search, view, or generate reports, or allow the user full ability to modify Floor plans for an entire Building.

Username and Passwords

Standard customer access is a username and password, entered through the Web browser on a user's system.

- Each CenterStone username has a unique security policy assigned to it, where risks and patterns can be defined and determined by the customer. Only a single instance of any username session can access the application and data at any time.
- All passwords are stored encrypted, to reduce the chances of a security breach. Additional methods of authentication are available in the form of RSA Secured cards or client certificates.
- Administrators have considerable control over user passwords, including
 - setting passwords to expire in specific timeframes (for example, 30 days).
 - forcing users to change their passwords when they log in to the application.
 - requiring a combination of letters and numbers for passwords.
 - forcing passwords to minimum/maximum lengths.

Manhattan CenterStone can customize CenterStone to add any additional password requirements required by a customer.

- CenterStone includes history tracking of used passwords, so passwords are not re-used.
- CenterStone includes the ability to lock users out of the application after a specified number of login failures.

The Client Applet

Users gain access to the application via the CenterStone Applet, a pure Java applet that employs Sun Microsystem's Java Plug-in version 1.4.2. The user types a specific URL as the browser address, which invokes the applet. The Java plug-in opens a "sandbox" or "virtual machine," which is a set of computer resources and instructions that make up the environment for the applet's execution. The CenterStone Applet attributes are:

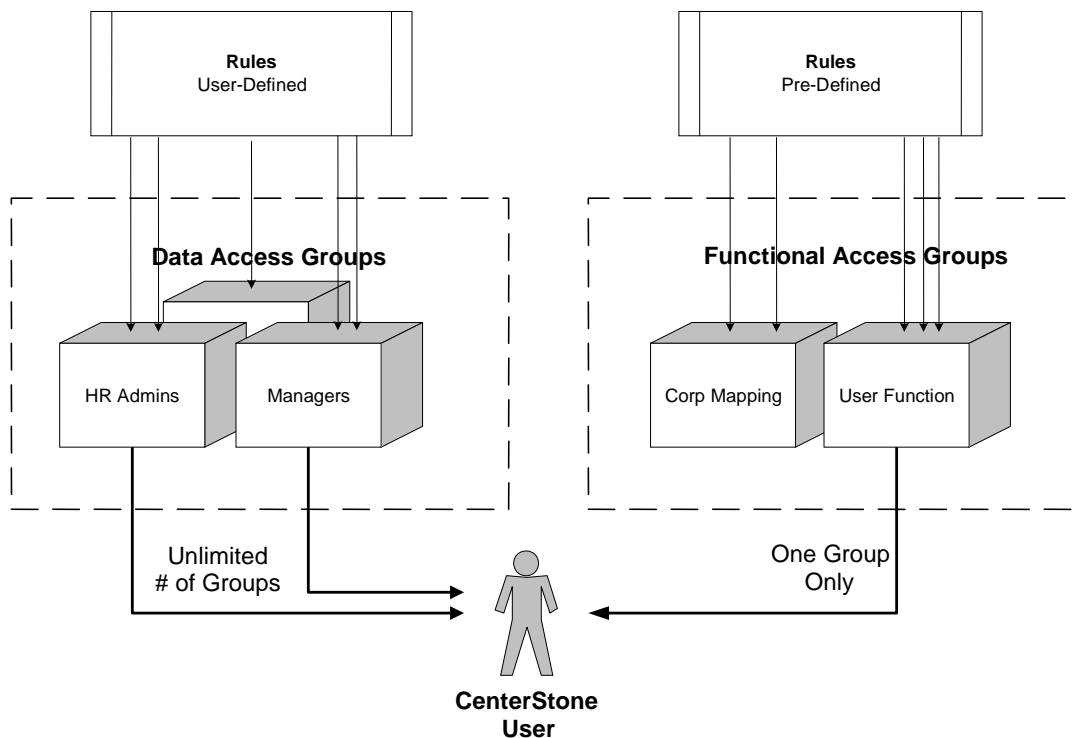
- It runs within the standard Java Runtime Environment as pure Java code. This means that CenterStone conforms to the ideal of universal portability, as a platform-neutral application.
- It is a Signed Java Applet. For security reasons, standard Java applets do not have permissions to access local resources and thus cannot execute software on the client machine. To overcome this, both Netscape's Communicator and Microsoft's Internet Explorer allow applets to be digitally signed with a private key associated with an RSA object-signing certificate. If the user accepts the certificate, therefore trusting the applet, then the browser allows the applet access permissions outside the Java security sandbox. Communicator and Internet Explorer implement different methods and technologies for digitally signing and distributing objects.
- CenterStone employs a 'plug-in' architecture that uses Sun Microsystem's Java Plug-in version 1.4.2 to view the Applet. Any certificate accepted by the user grants universal access to local system resources.
- It does not use any ActiveX technology in its architecture or implementation. ActiveX controls are fully executable pieces of Windows code that have no restrictions placed on them once they reach the client machine, regardless of how they got there. ActiveX controls may also compromise system security to if their origin and certifications are unknown.
- It only uses Port 443 (SSL) or Port 80.
- It will function properly through any installed proxy servers and/or firewalls, provided there is no restriction to the client for web access.
- Each time it is executed, it automatically performs a version check against any already existing CenterStone applet, and downloads a newer version when necessary.
- Parts of CenterStone, such as Corporate Mapping, utilize JSP pages only and do not require the Java Plug-in.

Functional & Data Access Control Security

Within the CenterStone application, Manhattan CenterStone provides functional and data access control security for both customer data and user access to that data. The security is configured in the application through the User Management options of Rules, Groups (functional or data access), and Users, and the Setup option related to Custom Searches. CenterStone Administrators monitor and modify all information relevant to Users, Groups, and Rules with this functionality.

The first security decision applies to the data, in the form of access control *Rules*. Rules are access control levels (*Read, Read/Write, Read/Write/Delete, None*) for the data *fields* and/or data *values* in the CenterStone data tables. Once a Rule is defined, it may be applied to one or more Data Access Groups.

CenterStone Access Controls



The *Functional Access Groups* (for example, Full Admin, Administrator, Corporate Mapping) determine which functional tabs, or parts of the application, a User may actually see or have access to in his or her CenterStone sessions. Each Group has a set of *pre-defined* Rules associated with it, all of which apply to any User who is a member of the Group. Users may be assigned to only one Functional Access Group, and the Administrator may move Users from one Access Group to another as the need arises.

Each *Data Access Group* (for example, Asset Readers, Building Contractors, HR Administrators, VP) determines the access control level a User has to the CenterStone data tables (Assets, Human Resources, Business Units, Structural Units, Operations Management, Project Management, Leasing). Each Data Access Group has a set of *customer-defined* Rules associated with it, all of which apply to any User who is a member of the Group. Users may be assigned to as many Data Access Groups as are appropriate by the customer security policies and standards.

Data Imports

CenterStone is designed for flexibility when creating or updating customer data. The Import functionality facilitates ease of data entry, while at the same time maintaining high standards for security integrity. Customers have the option of not only importing new or updated data into an existing database on a manual, record by record basis, but they may use batch importing when large numbers of records are involved.

All CenterStone data imports and exports are based on using Simple Object Access Protocol (SOAP). SOAP is an XML-based protocol that consists of an envelope that defines a framework for describing what is in a transmission and how to process it, a set of application-defined encoding rules, and a convention for representing remote procedure calls and responses. The standard formats for CenterStone data import/export are XML, standard ASCII text, and Excel spreadsheets (.XLS). All importing and exporting takes place over encrypted SSL.

Hosting Environment

Manhattan CenterStone has partnered with Computer Sciences Corporation, Inc. (CSC) to provide superior hosting and security to Manhattan CenterStone's clients.

CSC, one of the world's leading information technology services providers, helps organizations achieve business results through the adroit use of technology. No other company offers the same range of professional services and global reach as CSC does in areas such as e-business strategies and technologies, management consulting, information systems consulting and integration, application software, and IT and business process outsourcing.

CSC's global managed hosting service sets very high standards for security. Their INFOSEC group is one of only four companies authorized by the U.S. government as commercial evaluators under NIAP (product and system evaluations in accordance with International Common Criteria). Further, CSC is the first of only three organizations to earn the Software Engineering Institute's Capability Maturity Model (CMM) Level 3 rating for its information security assessment methodology.

Manhattan CenterStone's decision to partner with CSC is based on the commitment to providing customers with security management best practices in the web-hosted application space. CSC's managed hosting solution extremely exhibits high levels of performance in its class across the industry, and improves Manhattan CenterStone's ability to provide customers with secure, affordable applications that can keep pace with a rapidly expanding and complex technology.

Included in this managed hosting service is the core infrastructure required to host the CenterStone application. The core consists of the switches, firewalls, routers, and other equipment (such as load balancers) comprising the security and network infrastructure. The infrastructure is designed with no single points of failure, in order to meet high availability requirements. Manhattan CenterStone's application executes load balancing on a per session basis. When users log in, the application checks available resource pools, and determines at the point of login which pool is appropriate for handling the login.

CSC's security services protect the code and data contained in the CenterStone environment, and its security policy requires corresponding monitoring and access controls be applied to both people and processes accessing the environment. The approach of CSC's security framework focuses on building a secure foundation (prevention) with appropriate state-of-the-art monitoring tools (detection), backed up by solid incident management processes (reaction).

The CSC Hosting Solutions network architecture complies with the following network requirements:

- Built-in network infrastructure redundancy
- Web Server health checks

- Network infrastructure optimized for high availability
- Redundant path and carrier ISP access
- End user and customer access to CSC hosting systems over the Internet
- Connection to existing enterprise systems through secured links (private line management to demarcation within customers data center)
- Managed WAN connections
- Intrusion Detection Systems for real time security monitoring
- Shared or dedicated architectural solutions to meet client requirements
- Event and Performance monitoring of all production systems

CSC's Hosting Solutions incorporate a robust, redundant, high-speed, and high-availability network architecture that provides reliable, powerful service.

The CSC Hosting Solutions Network is designed for growth, capacity, and 100 percent availability, and has the following features:

- The core backbone at each CSC web hosting center is connected directly to tier-one service providers for direct Internet access. This access is available through high-speed circuits that can be easily expanded to support the necessary service and capacity.
- Multiple paths from CSC Web hosting centers extend to tier-one providers for additional levels of internetworking paths and redundancy. The CSC Web hosting centers interconnect over a high-speed, private internetwork that provides further levels of redundancy and service. CSC continually monitors all internetworking links for availability and capacity as a standard part of the service offering.

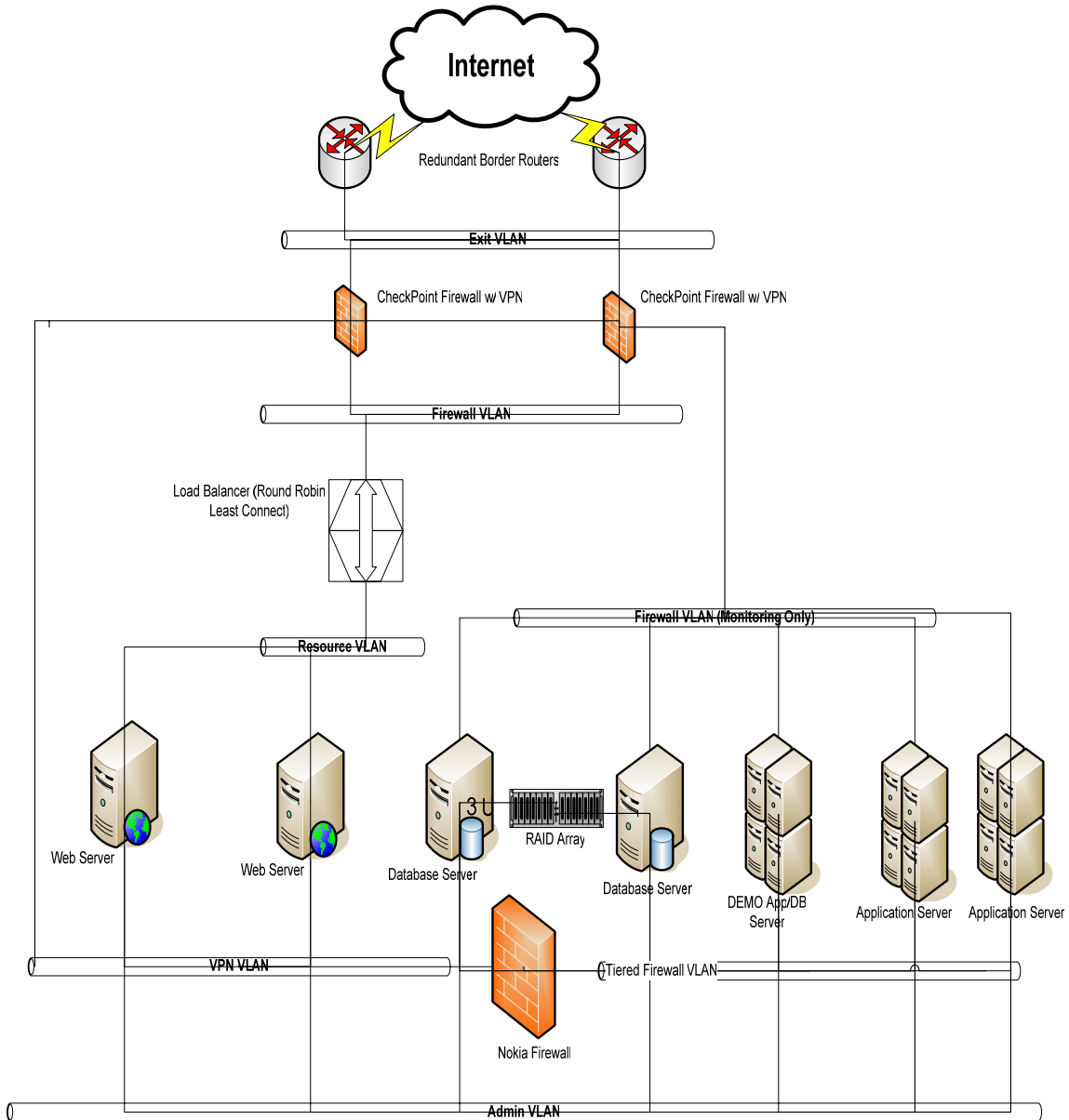
For those customers who wish to self-host CenterStone at their own enterprise-wide network operations and data centers, Manhattan CenterStone Client Services and Consulting staff can assist in providing configuration and security setup parameters and implementation guidance.

Managed Hosting Center (Data Center)

CenterStone is hosted in CSC's Cambridge facility. CSC's Web hosting centers provide premium site-hosting facilities. Each CSC Web hosting center has the following basic features:

- Manned security at multiple levels, 24 hours a day
- HVAC-power and an uninterruptible power supply
- Commercial power from two separate grids, each of which has multiple generating facilities
- Backup substation available to the substation supplying power to the complex, located on a common bus with the main substation
- Video-camera surveillance
- Monitored fire and smoke detection and suppression
- Connectivity to multiple telecommunications service providers, as well as to customer's internal WAN (intranet)
- Alternate sites in the event the primary site becomes unavailable or uninhabitable due to a disaster

CenterStone Hosted Architecture



Note: The front end firewall supports public access only to the Public VLAN. Access to the Management VLAN is only for CSC access (to allow monitoring and system management). All network traffic from the Public VLAN to the Application Server is routed through the Private VLAN and the second firewall.

SAS 70 Compliance

CSC conforms to the Statement on Auditing Standards (SAS) No. 70, *Service Organizations*, an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). In today's global economy, CSC recognizes that service organizations or service providers must demonstrate that they have adequate controls and safeguards when they host or process data belonging to their customers. A SAS 70 audit or examination is widely recognized, because it represents that a service organization has been through an in-depth audit of their control activities, which generally include controls over information technology and related processes.

As of the current date, CSC's Cambridge data center has been audited for SAS 70 compliance.

Network Security Architecture

Firewalls

A firewall normally prevents unauthorized personnel from getting access to a company's network through the global Internet, and can also prevent or control users from getting out to the Internet from an internal local network. Firewalls exist as a combination hardware/software buffer located between internal networks and the Internet. This buffering protects the internal network from intruders or hackers who might try to use the Internet to break into those systems.

The main function of any firewall is to regulate access between networks based on pre-determined security policies. Only specific kinds of messages from the Internet are allowed to flow in and out of the internal network. To enable information to travel in and out of a protected network, holes or "ports" must be opened in the firewall. Manhattan CenterStone uses only port 443 (Secure Socket Layer, or SSL), or port 80.

The three main categories of attacks against an internal network can be classified as:

- Intrusion.
- Denial of services.
- Information theft.

With intrusion, hackers are able to access private resources such as computers, network bandwidth and network accounts illegally.

A denial of service attack prevents legitimate users from accessing or using their own resources. For instance, if your server is being attacked by SYN flooding, it will be flooded by connections to numerous virtual clients so that legitimate clients will not be able to access the services provided by the WWW server. Although denial of services attack will not corrupt your data, clever attackers can disable your services and replace them with their virtual services.

The last category of attack is information theft. Hackers may either crack into users' accounts or "peek" into accounts for sensitive information. They may use network traps, which are usually called *sniffers*, for gathering private information such as bank account information, credit card numbers and network security passwords.

For this reason, Manhattan CenterStone has implemented a robust, secure architecture and strong security policy. Manhattan CenterStone's tiered firewall configuration is the only access into CenterStone, and the hosted architecture allows for client scalability and administrative flexibility.

CSC manages the Checkpoint firewalls for Manhattan CenterStone's hosting environment, and the CSC internal Site Patrol team monitors and manages the firewalls on a continuous basis from their Network Operating Center. Site Patrol includes a reliable and proprietary event monitoring system that automatically generates log information in the event of intrusion or suspected compromise. The logs capture data on all traffic passing through or denied by the firewall, which is then reviewed by experienced CSC staff, thereby ensuring system integrity. Content security extends security management to include anti-virus scanning, Java and ActiveX security, email content security, and URL categorization, reporting, and filtering.

Encryption

Manhattan CenterStone has a well-defined policy regarding software encryption:

- Symmetric encryption keys (for example, DES) used in data transmissions are changed once every six months, or immediately, if a compromise or breach is suspected. Asymmetric key pairs and associated certificates are reviewed on an annual basis and regenerated if the algorithms are no longer considered strong, in accordance with industry standards.
- Digital certificates are revoked immediately if a compromise or breach is suspected. It is possible for Manhattan CenterStone to use client certificates, if the client requests this.
- A secure process is used for the storage, distribution, and destruction of encryption keys.
- All transmission on the Internet is encrypted. The key length at all times meets or exceeds industry standards for strong encryption. 128-bit encryption is roughly 309 *septillion* times stronger than 40-bit encryption.
- All CenterStone accounts are set up with 128-bit encryption (SSL), unless the client in writing declines the use of encryption. Additionally, Manhattan CenterStone can force 128-bit encryption at the client's request.
- No transmissions between CenterStone servers and authorized Manhattan CenterStone workstations (high security systems only) are permitted other than through a Secure Remote VPN, using 128-bit encryption.

OS and Security Patching & Hardening

The first step towards safeguarding systems from intrusion is making sure that the operating system is up to date with the most recent recommended OS and security updates. Workstations and servers typically arrive installed with a multitude of development tools and utilities, which, although beneficial, also provide potential back-door access to an organization's systems.

Hardening of the operating system involves the removal of all non-essential tools, utilities and other systems administration options, any of which could be used to ease a hacker's path to client systems. The hardening process ensures that all appropriate security features are activated and configured correctly.

CSC builds the Managed and Customer Managed Hosting Services on top of a standard hardware and software platform called the Common Hosting Platform (CHP). Manhattan CenterStone's hosting solution combines these standard components in order to create a customized server. The CHP provides a uniform security model, so that Manhattan CenterStone realizes increased performance, security, reliability, ensuring that all configurations use fully-tested and authorized software and hardware.

All OS and security patches are pre-certified by CSC before application to the CHP and Manhattan CenterStone's servers. Further, Manhattan CenterStone applies the same patches to their testing systems to ensure that they will not cause adverse or undesirable effects in the CenterStone application.

Along with security patching, Manhattan CenterStone reserves the right to apply patches for the CenterStone product without notice between the hours of 11:00 PM – 2:00 AM EST, Wednesday and Saturday. All other outages to update the CenterStone product will be communicated to all our clients via our client notification list at least one week in advance.

Active Network Monitoring and Intrusion Detection

Manhattan CenterStone relies upon CSC's Network Intrusion Detection Services. This service consists of the deployment and operation of intrusion detection and monitoring tools at sensitive network entry points.

CSC uses Network Flight Recorder's (NFR) Network Intrusion Detection Sensors (NIDS), which are network-based probes that monitor traffic and compare it against known attack signatures. CSC's staff continuously monitors Manhattan CenterStone's environment for malicious or unauthorized activities. CSC intrusion detection is based primarily on predictive monitoring, rather than reactive procedures, following a network compromise or breach.

When unauthorized access attempts are detected, CSC security operations staff is alerted and they then start the Security Incident escalation procedures to mitigate the presented threat in a timely, appropriate way.

CSC's monitoring technology and staff helps to ensure that Manhattan CenterStone's servers and Internet connections are continuously accessible and reliable. These monitoring services include OS Monitoring of the Common Hosting Platform (CHP), including the backup clients. This provides fault detection and verifies whether the operating system is functioning.

External Audits

Manhattan CenterStone recognizes the distinction between penetration testing and network security assessments. Network security or vulnerability assessments may be useful, but they do not always reflect the extent to which malicious individuals will go to exploit or compromise a system. For example, recent studies have concluded that Denial of Service (DoS) attacks cannot be truly prevented.

Predictive Systems

CSC bases its security model on predictive systems, that is, methods and procedures that anticipate intrusion scenarios, and block them before they can compromise the network. Routine elements of the predictive systems include

- Packet filtering on all routers
- Active intrusion detection monitoring
- Denial of Service monitoring
- Regular security reports to Manhattan CenterStone .

Manhattan CenterStone augments the predictive security model through CenterStone's functionality, which includes

- Logging of all user login attempts
- Logging of all user sessions, which details
 - how long each user remains in the application
 - the IP address from which each user logs in
 - what type of operations they performed while using CenterStone (for example, submitting service requests, working with Floor plans, modifying Human Resource records).
- Additional logging may also be configured for each database write operation, including
 - what data the user is modifying
 - the values of data before and after any modification.

- Use of SPI Labs, Inc.’s WebInspect tool to ensure that any vulnerabilities are found and corrected at the source, before any system compromises occur. WebInspect identifies both known vulnerabilities common to the technology components as well as the critical vulnerabilities unique to that integrated system including detailed remediation reports. The WebInspect product combines signature-based scanning of static “known” vulnerabilities with adaptive heuristics technology, allowing it to identify a vulnerability unique to Manhattan CenterStone’s web application, whether coming from the application, configuration errors, or a misconfigured network architecture.

Network Penetration Tests

Penetration tests identify vulnerabilities in systems or networks that have existing security measures in place. Tests of this nature normally use invasive or malicious intrusion and hacking techniques, and are conducted by trusted individuals. In simple cases, a penetration test may involve scanning IP addresses to identify machines that are offering services with known vulnerabilities. In more thorough tests, testers might actually attempt to exploit known vulnerabilities that exist in unpatched operating systems. The results of penetration tests help system and network owners resolve any inconsistencies or weak points in their security implementation.

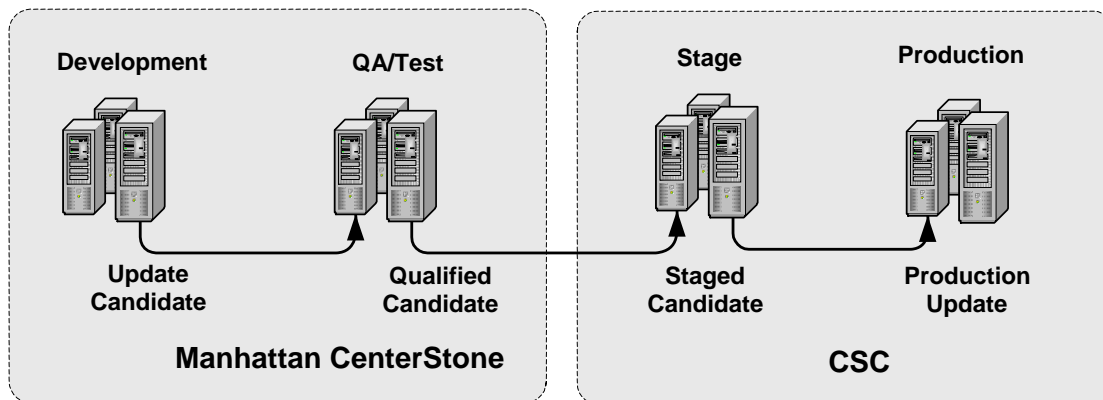
While penetration tests may be useful initially for establishing security procedures and shoring up defenses against intrusion, they are really nothing more than a "snapshot" of a system's security at a single moment in a specific time-frame. As such, they cannot and should not be referenced as an on-going portrait of a system's assessment. Further, penetration tests can have serious effects on the networks where they are conducted. In some cases, networks can be congested to the point where they will not function, or so overloaded by the test traffic and activity they actually crash. In a few cases, penetration tests can induce exactly the results security-minded customers are trying to avoid.

Another consideration is that there are security problems which such tests cannot identify. Often, the testers will not have complete information about the system being tested. The test can only identify those problems it is designed to seek out. A penetration test is unlikely to provide information about new vulnerabilities, especially those discovered after the test is carried out.

For these reasons, Manhattan CenterStone does not routinely conduct such tests, although it agrees to reasonably facilitate the efforts of customers whose management processes periodically require such tests. In fact, some of Manhattan CenterStone's customers have performed their own security audits which include penetration testing and ethical hacking, a few of which have been through the services of third-party commercial auditors, in order to satisfy their own requirements for system security. Manhattan CenterStone has been both willing and able to provide the customers and their auditors with assistance in setting up the test environments, executing the tests, and analyzing the results.

Application Updates

Manhattan CenterStone uses staged servers and a well-secured release process to deploy its CenterStone updates to customers. This staging provides a clean separation of development environments from release candidate environments, and ensures that customers do not acquire unvalidated components by virtue of having access to development repositories. Such staging is essential for a networked, web-centric application with a centralized web server and application server environment, such as CenterStone is.



CenterStone Staging Process

The staging area is set up as a delivery point that only contains tested, certified releases. Manhattan CenterStone's staging area replicates production configuration settings and system architecture and security. At each step of the application update, the code is securely under Manhattan CenterStone's control. Once a release candidate is validated for customer use, release engineers migrate the candidate components from the test servers to the staging servers, and finally to the production servers.

Once the staging is set, before any updates are committed, Manhattan CenterStone runs a standard set of configuration acceptance tests on the staging servers and production servers to ensure a successful deployment. The application itself is moved from the staging area to the production area(s) along a secured, encrypted access.

Backup and Disaster Recovery

Manhattan CenterStone takes active, positive steps to be certain that its systems are constantly monitored, updated and backed up. Offsite server and database backups ensure data and system integrity even in the event a disaster cuts off or damages an existing data center. As an additional level of recovery service, Manhattan CenterStone takes the concept of disaster recovery one step further by partnering with Raindrop Information Systems, an independent hosting sites located in London, England. By having CenterStone running at both of these providers it is possible to recover from even a major catastrophe, including a total shutdown of any individual hosting provider, within 24 hours.

Data Storage and Backup Procedures

Manhattan CenterStone, in conjunction with CSC, has defined backup and storage procedures that have a frequency range to insure that in the event of total disaster there is an effective backup and retrieval process to restore a customer environment with minimal, if any, data loss.

A backup process covers all of the various servers, files and data that encapsulate a CenterStone solution. A CenterStone solution contains three physical servers: web-server, database server and application server.

A backup contains three levels of software files: the CenterStone database, associated data files and system files.

A backup occurs on a scheduled basis such as nightly, weekly or monthly and includes the CenterStone database (containing the CenterStone data set) and any file stored in the CenterStone application (such as CAD drawings, scanned images of leases and spreadsheets) as well as security and administration data.

Backup Frequencies

CSC provides daily (incremental) and weekly (full) server backups to tape using a centralized Legato backup services. Weekly backups are rotated off-site and are transferred daily in secure lock boxes to climate-controlled vaults managed by Iron Mountain, Inc. The full disk backups for the last week of the month are retained offsite for a one-year period. Following the retention period, CSC's personnel degauss and reformat all retention media, so that data security is ensured.

File system backups are selected for each storage device based on the size of the customer-usable space available (a storage device is defined by CSC as a device

requiring a backup client). In addition, each server has a disk-shadow system for real-time back-ups. The backup level used is *RAID V*.

Beyond the database backup that is performed by the Legato system at CSC, Manhattan CenterStone performs an additional database backup-to-file to the local server, which is then backed up with the system files. This file is stored on the physical database server computer which runs at CSC. The benefit of this process is that the database information stored in the backup file can be restored to an intermediate file server and not directly to a server running a Microsoft SQL 2000 database. This enables Manhattan CenterStone to take the database backup file, after it has been restored to a file server, and move it to another data center and then restore the database data to another computer that is running a Microsoft SQL 2000 database. This provides Manhattan CenterStone with more flexibility to meet customers needs in both day-to-day and disaster recovery situations.

The weekly backup schedule runs from Monday to Sunday. At the end of each week, the backups are sent offsite, where they are held for one month.

System and data backup procedures are tested weekly, monthly, quarterly and yearly to ensure that backups are being properly created with no data loss and can be restored quickly and efficiently.

To provide another level of security, clients may request in writing that additional backups of databases be stored on CD media at a Manhattan CenterStone office location or directly at their own sites.

Standard Operating Procedures

Manhattan CenterStone recognizes its responsibility to ensure that data and information is safeguarded and secure in the event of a physical disaster, or hardware or software failure. Manhattan CenterStone has a standard set of operating procedures that form the basis of an emergency disaster recovery plan. These procedures are in place to insure that any request for a recovery, whether man-made, accidental or otherwise can be responded to with a large degree of redundancy and multi-level fail-safes.

A disaster recovery initiative focuses on two key areas: restoring the operating infrastructure and restoring the data. To address these areas, Manhattan CenterStone has a standard operational practice as follows:

- Within each hosting partner, Manhattan CenterStone has defined a fail-over process in the event of a physical site loss whether at the macro site level or at the server level.
- With its hosting partners, Manhattan CenterStone has implemented a multi-frequency and multi-location data backup procedure.
- Routine and scheduled testing of stored backups to insure complete data recovery

These standard operating procedures can be scaled based upon the significance of the disaster and recovery level experienced.

The priority of any recovery effort, regardless of the number of hosting sites and providers that Manhattan CenterStone may operate is to insure that a recovery occurs within an appointed site first, followed by redundant failover to secondary or tertiary sites and locations.

Manhattan CenterStone performs an annual test of its hosting centers backup and recovery processes to review all levels of the stated disaster recovery and data mitigation plans. This annual review is typically performed in the first quarter of any calendar year. Manhattan CenterStone's customers may request in writing to participate in any such review.

Secure Redundancy Using Multiple Hosting Providers

Manhattan CenterStone provides multiple levels of disaster recovery, both through the individual recovery features of a single hosting partner, and in addition, through the availability of multiple hosting partners. Most events can be addressed through a single hosting partner such as CSC. But, if for some reason CSC cannot estimate recovery of a Manhattan CenterStone customer after a catastrophic event within 24 hours, Manhattan CenterStone has the option and ability to restore a customers' data to a similarly configured set of servers at another hosting partner site.

Disaster Definition

Disasters and the required response to disasters are defined based upon the type of disaster experienced. Failures are categorized into four broad levels.

Minor condition

- Damage is confined to one service or machine (for example, a server, switch, or router), can be worked around by using off-site servers or hot-spare machines.

Major Condition

- Damage is localized to the data center; critical portions of service can be relocated to office spaces within the same building.

Catastrophic Condition (Level 1)

- A situation where there can be no use of the primary or nearby facilities, operations are transferred to another location.

Catastrophic Condition (Level 2)

- Similar to Level 1, but requires that data be moved from one hosting partner to another to achieve recovery.

When unforeseen events (a natural disaster, a fiber cut, a major power outage, or a fire at a data center) produce a major interruption of service, the CSC Emergency Broadcasting System (EBS) notifies Manhattan CenterStone staff within minutes. EBS alerts are delivered via pager, telephone, or fax about an extended network outage and provides instructions for obtaining further updates on the event. EBS uses the customer database to determine the contact and acceptable calling hours; if unsuccessful, EBS leaves voice mail with the alert and instructions for getting updates, then calls alternate numbers and retries as required.

All CSC office sites, Network Operation Centers (NOCs), data centers, and Points of Presence (POP) conform to documented CSC security policies. Standards provide national and company-wide security, loss prevention, and life safety protection.

Each data center utilizes our company standard access control system linked to our central Security Operations Center in Cambridge, MA. A local workstation is present at every site where security staff is located. The Cambridge data center has a 24-hour on-site contract security with a proprietary site supervisor. Security systems for CSC data centers are monitored by CSC security staff. An extensive CCTV system is installed in CSC's facility, including coverage down to the rack level.

General case checklists and recovery readiness verification timelines are shown below.

NOTE: *Disaster recovery is dependent upon the ability of Manhattan CenterStone to receive backup information from CSC. CSC and Manhattan CenterStone cannot guarantee a time period based upon uncontrollable conditions such as natural disasters, terrorism or deliberate sabotage. Manhattan CenterStone in conjunction with CSC will use best efforts to achieve recovery within the stated timeframes.*

Minor Condition Recovery

Example: Hard disk failure in the database server at the primary data center

| No . | Task | Estimated Time | Start Time | End Time | Comments |
|------|--|----------------|------------|----------|--|
| 1 | Notification of Event | START | | | |
| 2 | Confirmation of event and time to repair estimated | < 15 min | | | Manhattan CenterStone confirms severity of issue |
| 3 | If the issue will not cause system down time the issue is handled by Manhattan CenterStone staff. If the issue will cause system down time, the customer is notified of the issue. | < 15 min | | | If the repair estimate is under 24 hours and the repair does not require moving the customer's implementation to an alternate hosting site, the issue will be handled by CSC and Manhattan CenterStone. If not, please refer to Catastrophic Condition Recovery (Phase I) Step 4. |
| 4 | Disk is replaced and any necessary data is restored from on site backups | < 4 hours | | | Web/File server: D:\DWGFiles D:\E-CenterOneFiles D:\E-CenterOneLogon Database Server: D:\MSSQL\backups Application Server: D:\weblogic\myserver\EC1Files |
| 5 | Manhattan CenterStone performs Level 1 verification of data and application readiness | < 1 hour | | | Confirm that data has been updated to the backup system by high level review of data and functionality |
| 6 | Customer notification of initial system readiness for verification | < 10 min | | | |
| 7 | Restored system is validated and access is restored | END | | | |

Major Condition Recovery

Example: CenterStone server computer failure at the primary data center

| No. | Task | Estimated Time | Start Time | End Time | Comments |
|-----|---|----------------|------------|----------|--|
| 1 | Notification of Event | Start | | | |
| 2 | Confirmation of event and time to repair estimated | < 15 min | | | Manhattan CenterStone confirms severity of issue |
| 3 | If the issue will not cause system down time the issue is handled by Manhattan CenterStone staff. If the issue will cause system down time, the customer is notified of the issue. | < 15 min | | | If the repair estimate is under 24 hours and the repair does not require moving the customer's implementation to an alternate hosting site, the issue will be handled by CSC and Manhattan CenterStone. If not, please refer to <i>Catastrophic Condition Recovery (Phase I) Step 4.</i> |
| 4 | Manhattan CenterStone performs any necessary configuration to support proper function of the restored customers data and implementation | < 4 hours | | | Necessary tasks include: <ul style="list-style-type: none"> • Restore customer's database • Modify customer's policy table for new site • Restore customer's files • Add virtual director to IIS • Modify customer's login files • Modify customer's report files • Restore customer's home files to application server Add customer's database to connection pool. |
| 5 | Manhattan CenterStone performs Level 1 verification of data and application readiness | < 1 hour | | | Confirm that data has been updated to the backup system by high level review of data and functionality. |
| 6 | Customer notification of initial system readiness for verification | < 10 min | | | |
| 7 | Upon verification of the restored system the URL is rerouted to the new server and the system goes live Customers will be supplied with a temporary URL until the rerouted URL is propagated | END | | | Old URL: <a href="http://dr.ecenterone.com/<CustomerName>">http://dr.ecenterone.com/<CustomerName> > New URL: <a href="http://www.ecenterone.com/<CustomerName>">http://www.ecenterone.com/<CustomerName> |

Catastrophic Condition Recovery (Phase I)

Example: Fire at data center building

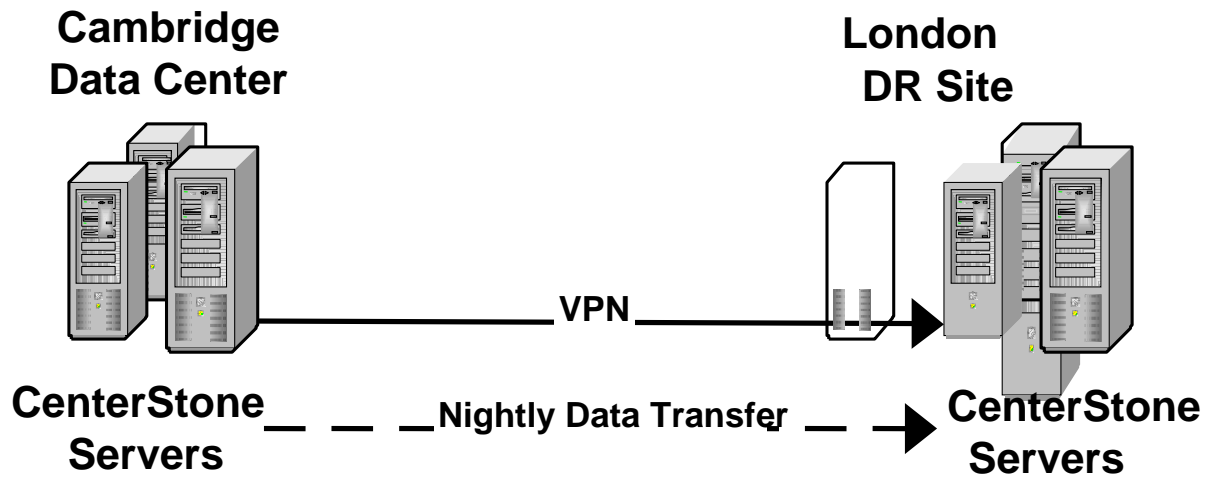
| No. | Task | Estimated Time | Start Time | End Time | Comments |
|-----|---|----------------|------------|----------|---|
| 1 | Notification of Event | Start | | | |
| 2 | Confirmation of event and time to repair estimated | < 15 min | | | Manhattan CenterStone confirms severity of issue |
| 3 | Customer notified of issue. | < 15 min | | | If the repair estimate is under 24 hours and the repair does not require moving the customer's implementation to an alternate hosting site, the issue will be handled by CSC and Manhattan CenterStone. If not, please refer to <i>Catastrophic Condition Recovery (Phase II) Step 4.</i> |
| 4 | A file server is designated at CSC and system software is restored. | < 18 hours | | | |
| 5 | Manhattan CenterStone restores backup files to the new servers at CSC | < 1 hour | | | <p>Web/File server: D:\DWGFiles D:\E-CenterOneFiles D:\E-CenterOneLogon</p> <p>Database Server: D:\MSSQL\backups</p> <p>Application Server: D:\weblogic\myserver\EC1Files</p> |
| 6 | Manhattan CenterStone performs any necessary configuration to support proper function of the restored customers data and implementation | < 2 hours | | | <p>Necessary tasks include:</p> <ul style="list-style-type: none"> • Restore customer's database • Modify customer's policy table for new site • Restore customer's files • Add virtual director to IIS • Modify customer's login files • Modify customer's report files • Restore customer's home files to application server • Add customer's database to connection pool |
| 7 | Manhattan CenterStone performs Level 1 verification of data and application readiness | < 1 hour | | | Confirm that data has been updated to the backup system by high level review of data and functionality |
| 8 | Customer notification of initial system readiness for verification | < 10 min | | | |
| 9 | Restored system is validated and access is restored | End | | | |

Catastrophic Condition Recovery (Phase II)

The following procedures will be implemented in the case of a *Catastrophic Condition* and if the decision is made to move the customer to an alternate hosting partner.

| No . | Task | Estimated Time | Start Time | End Time | Comments |
|------|---|----------------|------------|----------|--|
| 1 | Notification of Event | START | | | |
| 2 | Confirmation of event and time to repair estimated | < 15 min | | | Manhattan CenterStone confirms severity of issue |
| 3 | Customer notified of issue and restore options are discussed. An optimum solution is agreed upon between Manhattan CenterStone and the customer. | < 15 min | | | |
| 4 | Manhattan CenterStone performs any necessary configuration to support proper function of the restored customers data and implementation | < 4 hours | | | Necessary tasks include: <ul style="list-style-type: none"> • Restore customer's database • Modify customer's policy table for new site • Restore customer's files • Add virtual director to IIS • Modify customer's login files • Modify customer's report files • Restore customer's home files to application server • Add customer's database to connection pool |
| 5 | Manhattan CenterStone performs Level 1 verification of data and application readiness | < 1 hour | | | Confirm that data has been updated to the backup system by high level review of data and functionality |
| 6 | Customer notification of initial system readiness for verification | < 10 min | | | |
| 7 | Upon verification of the restored system the URL is rerouted to the new server and the system goes live Customers will be supplied with a temporary URL until the rerouted URL is propagated | END | | | Old URL: <a href="http://dr.ecenterone.com/<CustomerName>">http://dr.ecenterone.com/<CustomerName> New URL: <a href="http://www.ecenterone.com/<CustomerName>">http://www.ecenterone.com/<CustomerName> |

Catastrophic Condition Recovery (Phase II) Recovery Flow



Security Guidelines

CSC developed its standards from several sources of regulatory, legal, and corporate requirements, including:

- National Fire Prevention Association (NFPA) Requirements
- MEA (formerly BSA, BOMC) New City Standards
- CSC Corporate Security Standards and Procedures Manual
- Underwriters Laboratory (UL)
- California State Fire Marshall (CSFM)
- Other CSC documents, including: Protection of Assets Manual, Life Safety 101 Requirements, Factory Manual (FM).

CSC standards meet or exceed local rules, regulations, and requirements. The implementation of the physical security standards complies with Federal, state, and local statutory law.

Facility Security Standards

The Cambridge data center facilities are:

- Protected against damage from exposure to fire, water, and natural disasters
- Located away from hazardous processes or materials
- Located in geographical areas with low crime rates versus the national average

CSC's Cambridge data center enforces strict access control standards. Access to the facility is controlled by card-readers, with permission given to select CSC employees. Customers who wish physical access to their site must be escorted at all times by authorized CSC employees.

Glossary & Index of Terms

- **ActiveX** = software modules based on Microsoft's Component Object Model (COM) architecture. These modules provide developers with a way to download small executable objects that can be invoked directly on the users machine. These are fully executable pieces of Windows code that have no restrictions placed on them once they reach the client machine, regardless of how they got there. The only security provision is a digital signature system called Authenticode which offers only "run/don't run" options.
- **DoS** = Denial of Service.
- **Firewall** = A standard security measure composed of a system or combination of systems that enforce borders between two or more networks. A firewall regulates access between these networks based on security policies. To enable information to travel in and out of a protected network, holes or "ports" must be opened in the firewall.
- **HTTPS** = The secure hypertext transfer protocol is a communications protocol designed to transfer encrypted information between computers over the World Wide Web. HTTPS is HTTP over Secure Socket Layer (SSL). HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.
- **NIDS** = Network Intrusion Detection Systems. A technology that can be used to reduce the risk associated with extending the security perimeter. NIDS carries out two primary functions in VPN designs. First, NIDS can be used to analyze traffic coming from, or destined to, the VPN device. Second, NIDS can be used after encryption to validate that only encrypted traffic is sent and received by VPN devices.

NIDS monitor packets on the network wire to discover if a hacker/cracker is attempting to break into a system (or cause a denial of service attack). A typical example is a system that watches for large numbers of TCP connection requests (SYN) to many different ports on a target machine, thus discovering if someone is attempting a TCP port scan. NIDS may run either on the target machine which watches its own traffic (usually integrated with the stack and services themselves), or on an independent machine promiscuously watching all network traffic (hub, router, probe). Note that a "network" IDS monitors many machines, whereas the others monitor only a single machine (the one they are installed on).

- **RSA** = an encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman, founders of RSA Data Security, Inc. The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browser from Netscape and Microsoft, and many other products.

- **Remote Intrusion** = A hack involving an attacker who attempts to penetrate a system remotely across the network.
- **SOAP** = Simple Object Access Protocol. A lightweight protocol for exchanging information in a decentralized, distributed environment. SOAP is an XML-based protocol that consists of three parts: an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of application-defined datatypes, and a convention for representing remote procedure calls and responses. This allows programs running in one kind of operating system to communicate with a program in the same or another kind of an operating system by using the Web's Hypertext Transfer Protocol (HTTP) and XML as the mechanisms for information exchange.
- **SSL** = A secure socket layer is an encryption protocol invoked on a Web server that uses HTTPS. SSL allows software to communicate with Web servers in a secure, encrypted manner. Many web sites that conduct electronic commerce use SSL to securely transmit credit card numbers from a customer's Web browser to the Web server. SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.
- **VPN** = A virtual private network (VPN) is a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A virtual private network can be contrasted with an expensive system of owned or leased lines that can only be used by one organization. The goal of a VPN is to provide the organization with the same capabilities, but at a much lower cost.

A VPN works by using the shared public infrastructure while maintaining privacy through security procedures and tunneling protocols such as the Layer Two Tunneling Protocol (L2TP). In effect, the protocols, by encrypting data at the sending end and decrypting it at the receiving end, send the data through a "tunnel" that cannot be "entered" by data that is not properly encrypted. An additional level of security involves encrypting not only the data, but also the originating and receiving network addresses.

- **Vulnerability** = exploitable attribute of network node. May be hardware or software.

Confidentiality Notice

Manhattan CenterStone, Inc.

The information contained in this document constitutes valuable and confidential proprietary information of Manhattan CenterStone, Inc. (Manhattan CenterStone). No license to any technology or intellectual property rights of Manhattan CenterStone or their affiliates, subsidiaries, or their licensors is granted or to be implied through your receipt of this document.

You may use this document only in connection with your evaluation or use of the services that are the subject of this document. You may not otherwise use, and you may not reproduce, or disclose to any third party, this document or any of its contents without the express prior written consent of Manhattan CenterStone.

By accepting receipt of this document you agree to the above terms. If you do not agree to those terms, you must immediately return all copies of this document to your Manhattan CenterStone account manager, and you may not use any of the information contained in this document for any purpose.

Copyright © 2007 Manhattan CenterStone, Inc. All rights reserved. Other company and product names may be trademarks or service marks of their respective owners.