



TIB

The Independent BankersBank

Network and Internet
Security Model

Lyle Walden, Senior Vice President
Network Operations



End to End Security

- Desktop PC
- Modem
- Local Area Network
- Event Logging and Alerting
- E-Mail
- Router
- Firewall and DMZ
- Intrusion Detection
- Remote Access
- Security Layering
- Internet
- Compliance Auditing
- Change Control
- Websites and Mailing Lists



The Independent Bankers Bank

Desktop PC Security

Baseline Installation
Configuration Standards

Cloned Images for
Drop-in Setup

Baseline Security
Standards

Non-Routeable
IP Addressing



Desktop
Computer

Desktop Installed Antivirus
Software

Restrict Users From Installing
Software Locally

Windows NT, 2000, XP
for Separation of Admin Logons
Privileges and User Logons



The Independent Bankers Bank

Baseline Installation, Security and Configuration Standards

- Baseline Security Tools such as The Center for Internet Security's Security Scoring Tool should be used to ensure a standard Security Compliance for each PC.
- After successful scoring, the PC image should be imaged for repeat installation with an imaging tool such as Ghost.
- The Baseline Image should be used for all PC installations.



Desktop Restrictions

- Users should be restricted from installing any software.
- An Operating System such as Windows NT, 2000 or XP should be used to allow for segregated user and admin access.
- Users should be restricted to logging on to one workstation at a time.
- Login hours should correspond with normal hours of operation.



Network and PC Addresses

Personal Computer and File Server Network Addresses should be Non Internet Routable, such as:

192.168.xxx.xxx

or

10.xxx.xxx.xxx



Anti Virus

- Anti Virus Tools should be installed on each PC to periodically scan for malicious programs as well as scanning E-Mail.
- The software should be configured to scan upon any successful login.
- The software should be updated for new virus signatures automatically or manually each time they are releases from the Vendor.



Desktop PC Security Tools

- **CIS Security Benchmark and Scoring Tools**
 - <http://www.cisecurity.org/>
- **Ghost**
 - <http://www.symantec.com/>
- **Virus Protection**
 - <http://www.symantec.com/>
 - <http://www.mcafee.com/>
- **Personal Firewalls**
 - <http://www.consealfirewall.com/>
 - <http://www.zonelabs.com/>
 - <http://www.iss.net/>



The Independent BusinessBank

Modem Security



The Independent BusinessBank

Modem Security Best Practice

- Allow only Business to Business or Vendor Connections
- Actively Monitor the Connections
- If Internet Access is Via Modem, Actively use Anti-Virus and PC based Firewalls
- Allow Modem Connections on a Strict Case-by-Case Basis



The Independent BankersBank

Local Area Network Security



- Anti Virus Software installed on File Server
- Restricted File Access
- Password Policy
- Event Logging and Monitoring
- Disable all Ports and Services not Required for Business Operations
- Non Routable IP Addressing
- Baseline Security Defaults and Current Hosts/Patchlevels
- Periodic Review for Compliance of Access Rights, Ports and Services, and Hosts/Patchlevels



The Independent BankersBank

Local Network Security Tools

- Periodically Verify User Rights and File Permissions
 - <http://www.somarsoft.com/>
 - <http://www.hhdssoftware.com/srvadmin.html>
- Event Logging and Monitoring
 - <http://www.prismmicrosys.com/eventtracker/eventTracker-index.htm>
 - <http://www.eventreporter.com/en/Product/Forward-NT-Event-Logs-Via-EMail.asp>
 - <http://www.gfi.com/lanselm/>
- Run only the services and ports needed for server operation
 - <http://www.iana.org/assignments/port-numbers/>



Local Network Security Tools

- Virus Protection
- Non Routable Private IP Addresses
- Hotfix and Patchlevels
 - <http://www.codeproject.com/tools/whotfixcheck2.asp>
 - <http://www.maximized.com/>
 - <http://support.microsoft.com/default.aspx?scid=KB;EN-US;q303215&>
- Baseline Security Standards
 - <http://www.cisecurity.org/>
- Password Policy



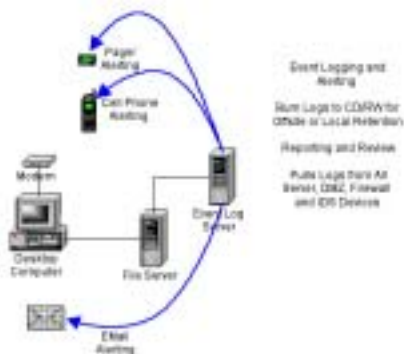
Local Network Security Tools

- Enforce a Stringent Password Policy
- Perform Periodic Review for Access and File Permission Rights, Ports and Services, and Hotfix, Service Pack and Patchlevels



The Independent BankersBank

Event Logging And Alerting



The Independent BankersBank

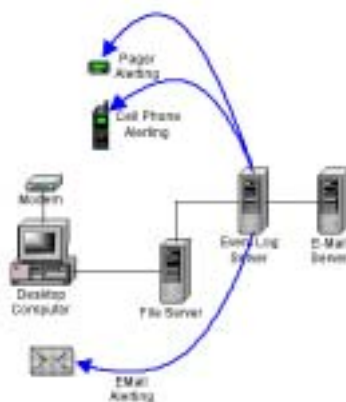
Logging, Alerting, Reporting and Retention

- All logs should be forwarded to a logfile server
- Copy the logs to CD or Tape Every 30 Days
- Store them Offsite or Onsite in a Fireproof Safe
- Logs should be reviewed daily and reported monthly

Logging Software and Tools

- Kiwi
 - <http://www.kiwisyslog.com/>
- Logcaster
 - <http://www.ei-europe.com/logcaster.htm>
- Languard SELM
 - <http://www.gfi.com/>

E-Mail Security



- Anti-Virus Software installed on File Server
- Content Filtering
- Restricted File Access
- Event Logging and Monitoring
- Disable all Ports and Services not Required for Business Operations
- Non Realistic IP Addressing
- Baseline Security Defaults and Current Hotfix/Patchlevels
- Periodic Review for Compliance of Access Rights, Ports and Services, and Hotfix/Patchlevels
- Encryptor



Anti Virus and Content Filtering

- McAfee
 - www.nai.com
- Norton Anti Virus
 - www.symantec.com
- Webshield
 - www.nai.com



Encryption and Encryption Tools

- PGP
 - <http://www.pgp.com>
- HandyBits EasyCrypto
 - <http://www.handybits.com/>



The Independent BankersBank

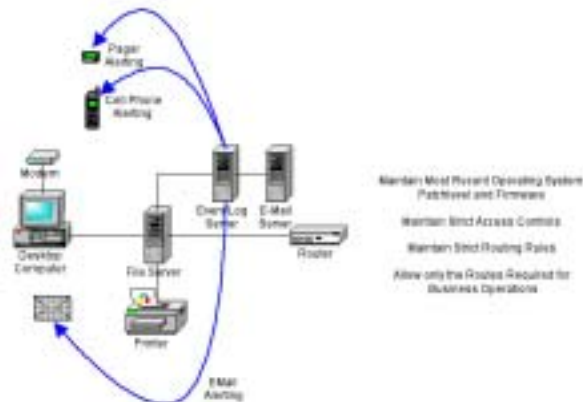
Ports, Services and Periodic Review

- All unneeded ports and services should be turned off in order to ensure the potential for misuse is minimized.
- All systems should receive a periodic review to ensure they remain current with compliance and security standards.



The Independent BankersBank

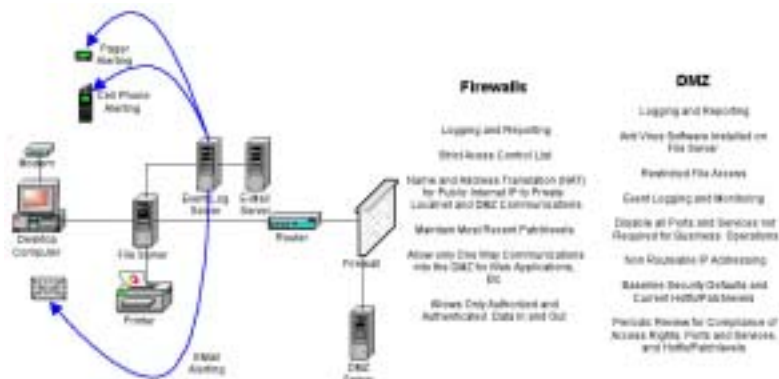
Router Security



Router Security

- Routers should be periodically checked to ensure they are using the most current firmware version.
- Access controls should be maintained to prevent unauthorized traffic across the network.
- Routing tables must be maintained to prevent a disruption in network services

Firewall and DMZ Security





Firewall and DMZ Security

- All network perimeter connections to the Internet should be protected with a firewall device.
- All necessary communications from the Internet to an internal network should occur in a DMZ environment.
- In some cases, it is recommended firewalls be installed on internal networks for access to information that is sensitive or is of monetary value.



Firewall and DMZ Security

- All firewall logs should be forwarded to a logging server and should be reviewed daily and reported at least monthly.
- A very strict access control list should be maintained to minimize the risk of unauthorized access or malicious use.
- Name and Address Translation from public to private IP space should occur at the firewall.



Intrusion Detection

- Intrusion Detection devices listen to all incoming and outgoing traffic.
- Some intrusion detection systems have the ability to drop malicious or suspicious connections.
- Intrusion detection systems should forward logs to a logging server for review and reporting, and provide alerting based on user setup criteria.



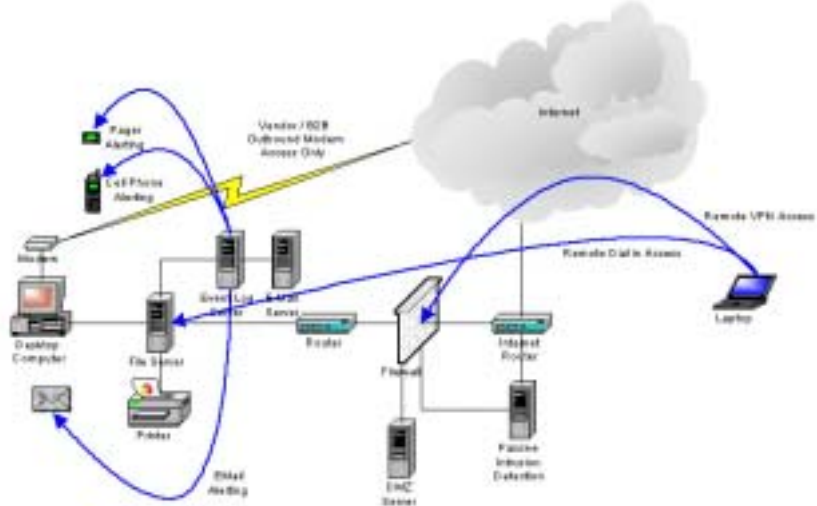
Intrusion Detection Software

- ISS Realsecure
 - <http://www.iss.net>
- Snort
 - <http://www.snort.org>
- NetProwler
 - <http://www.symantic.com>



The Independent BankerBank

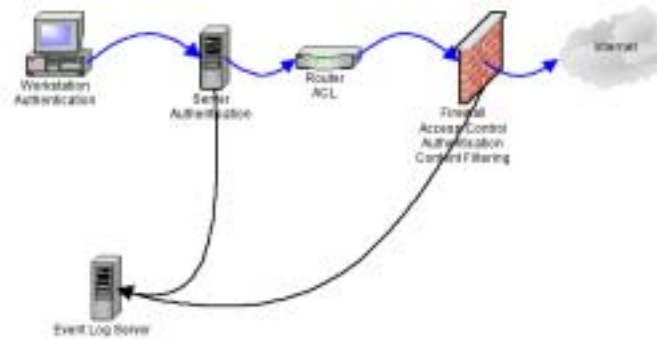
Basic Network Security Model



The Independent BankerBank

Internal Security

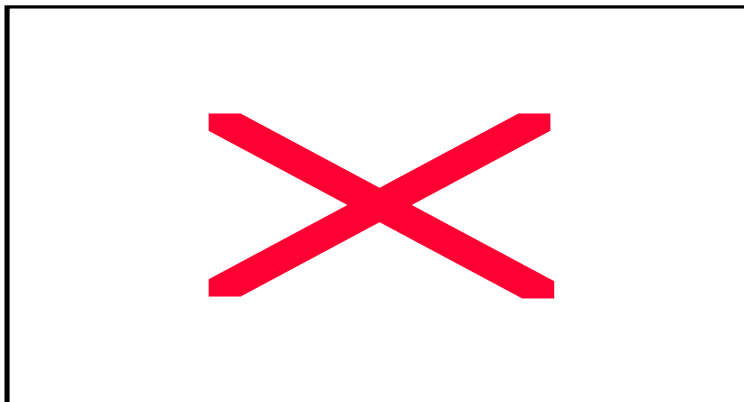
Internal Access Layering



Internal Access Layering

- Internal access layering is the process of requiring multiple authentication points.
- Users must log in to their desktop computers, authenticate to the server, be part of an access control list to access the firewall, and have rights on the firewall to access the Internet based on service and content filtering rules. This activity is logged at the server and the firewall.

Internet Security





External Access Layering

- External security layering is initiated for several reasons. Legitimate users, consumers and malicious users all want to access Internet servers and information.
- By layering accessibility to external interfaces, exposure is reduced to a minimum.



External Access Layering

- RAS dialup users must know the call in number, must know a username and have a password. Services are restricted to only those that are absolutely required.
- VPN users must authenticate with a username and password to the VPN concentration point, must have rule based firewall rights to allow the internal network, username and password on servers, and services are restricted to only those that are absolutely required.



External Access Layering

- Consumers are only allowed access to DMZ secured servers by firewall rule and information is limited. Unless financial transactions or sensitive information occur no password or username is required.
- Intrusion Detection equipment watches for and filters malicious port connections, only connections with proper port destinations are permitted to reach the firewall.



External Access Layering

- Firewalls inspect connections passed by the intrusion detection devices and determines their destination based on the firewall rules.
- All external connection attempts and activity are logged, reviewed and reported.
- Alerting can take place from the intrusion detection device, firewall or logging server.



The Independent Bankers Bank

Security and Compliance Auditing

- All network devices should be routinely audited for compliance and security related issues.
- Security audits and scans should be scheduled and notifications given to anyone that may be affected by the scans.
- Any hotfixes, service packs or patches required should be scheduled and if possible, tested before implementation.



The Independent Bankers Bank

Security and Compliance Auditing Tools

- Nessus
 - www.nessus.org
- Retina
 - www.eeye.com
- CIS Baseline Security Tool
 - www.cisecurity.com
- Languard Network Scanner
 - www.gfi.com



Change Control

- All network infrastructure changes should be discussed and tested before any implementation.
- Changes should be scheduled for non business hours in order not to impact users, customers or interrupt the flow of business
- Everyone impacted by any change should be notified well in advance of implementation.



Security Related Websites and Tools

- <http://www.packetstormsecurity.com/>
- <http://www.securityfocus.com/>
- http://www.hideaway.net/home/public_html/index.php
- <http://www.securiteam.com/>
- <http://www.net-security.org/>
- <http://news.ists.dartmouth.edu/todaynews.html>
- <http://incidents.org/>
- <http://www.phrack.org/>
- <http://archives.neohapsis.com/archives/bugtraq/>



The Independent Bankers Bank

Security Related Mailing Lists

- SecurityFocus/Bugtraq
 - <http://www.securityfocus.com>
- NT Bugtraq
 - <http://www.ntbugtraq.com>
- SANS
 - <http://www.sans.org>
- CERT
 - <http://www.cert.org>
- ISTS
 - <http://news.ists.dartmouth.edu/>
- NIPC
 - <http://www.nipc.gov>
- Vulnwatch
 - <http://www.vulnwatch.org>



The Independent Bankers Bank

Conclusions

- Network Security is dynamic and reactive.
- Following sound prevention guidelines will eliminate the majority of risk present in most network infrastructure.
- Keeping abreast of current security information and notices is critical to preventing intrusions, loss of business, information and financial data.
- Security isn't just a firewall, it's an end to end process that requires management, oversight and due diligence.