Security and Audit Considerations in a Telecommuting Environment

April 10, 2008

Agenda

- **Introductions**
  - Bryan McGowan
  - Clint Newell
- **Telecommuting Definition and Facts**
- **The Telecommuting Environment**
  - What can companies and telecommuters do to protect sensitive data and mitigate risks in a telecommuting environment?
- **Questions and Answers**

Telecommuting Definition and Fun Facts

- **Definition**
  - Telecommuting – Working from a remote location rather than commuting via automobile or other mode of transportation to and from an employer's work site to perform equivalent work

- **Fun Facts**
  - Last year an estimated 8.9 million people worked from home three or more days each month. A quarter of them worked exclusively from home (IDC)
  - If 10 percent of the workforce would telecommute once a week, more than 12 million gallons of fuel would be saved, resulting in 12,963 tons of avoided air pollution (ATA)

The Telecommuting Environment

- **Security Concerns**
  - Hardware theft
  - Unauthorized access (data on remote device)
  - Device configuration management
  - Remote access solutions
  - Remote access monitoring
  - Unauthorized access (corporate network)

- **Cost vs. Benefit of Telecommuting**

Hardware Theft

- **Facts**
  - An analyst's laptop and external hard drive from the Department of Veterans Affairs was stolen containing social security numbers of 26 million-plus veterans including their name and date of birth (CNN, May 2006)
  - More than 600,000 laptop thefts occur annually (Safeware Study, 2004)
  - A laptop computer containing sensitive, personally-identifiable information was stolen from an individual at a major data security company. The laptop contained current and past employee information and other sensitive company information. (Computerworld, Aug 2007)

Hardware Theft

- **Risks**
  - Inappropriate or illegal use of company or client data
  - Damage to reputation and company image
  - Additional costs to company for recovery of hardware
  - Unauthorized access to proprietary or sensitive data

Hardware Theft

- **Solutions / Audit Considerations**
  - Telecommuter Policy & Acknowledgement Form
  - Security awareness training
  - Protection while traveling (storage in car, handling in airport, carrying a discrete bag)
  - Use a security cable, label and tag the laptop
  - Data encryption and authentication (discussed in later slides)
    - Disk and file encryption
  - Hotline to report lost or stolen hardware
  - Ability to disable hardware remotely (PDA's)
    - Remote kill software
  - Device tracking (GPS)
  - Data backup
    - Real-time synchronization
    - Schedule periodic backups

Unauthorized Access to Data

- **Facts**
  - In the second half of 2006, theft or loss of a computer or data storage medium made up 54 percent of all identity theft-related data breaches (Symantec, 2007)
  - The estimated cost of one unrecovered PDA or mobile phone is approximately $2,500 per unit, because of the expense of compromised proprietary data (Gartner, 2007)

Unauthorized Access to Data

- **Risks**
  - Costs of retrieving, restoring, or recreating data
  - Costs of credit monitoring and other damage-control mechanisms
    - Reimbursement of losses
    - Notification to customers
  - Inappropriate or illegal use of company or client data
  - Damage to reputation and company image
    - Loss of revenue
    - Loss of customers
  - Company or client data being can used inappropriately or illegally

Unauthorized Access to Data

- **Solutions / Audit Considerations**
  - **Encrypt Data on Hardware**
    - File encryption vs. disk encryption
  - **Authentication Requirements**
    - Password rules
    - Biometrics
    - Password-protected screensavers
    - PDA lockout
  - **Access Controls**
    - File sharing policies
    - Data storage policies
    - Logical access restrictions

Device Configuration Management

- **Risks**
  - Required software updates are not installed (i.e. Virus Protection, O/S Patches)
  - Unauthorized software installation
  - Excessive permissions to the device
  - Unauthorized access to data and files
  - Inappropriate storage of data and files

Device Configuration Management

- **Solutions / Audit Considerations**
  - **Company Managed**
    - Pre-configure device to company specifications
    - Corporate IT supports devices
    - Update O/S and virus protection software through online distribution
    - Continuously monitor the usage of the device and software that has been installed
    - Restrict access, services, and hardware components
  - **Employee Managed**
    - Require telecommuter to sign acknowledgement of appropriate device management
    - Individual supports devices
    - Educate telecommuter on the purpose and benefit of firewalls, virus protection software and the data file storage policy
    - Require software updates for telecommuters
    - Establish disciplinary action for non-compliance
    - Add software at the corporate level to audit PC prior to granting access to the corporate network
    - Require firewalls and virus protection software

Device Configuration Management

- **Firewalls**
  - Firewall software
  - External hardware-based firewall
- **Virus Protection**
  - Updated virus dictionaries
  - Scanning tools
- **Operating System Patches**
  - Strengthen known weaknesses

Remote Access Solution

- **Risks**
  - DoS (Denial Of Service Attack)
  - Traffic interception
  - Network intrusion
  - Unauthorized devices on network

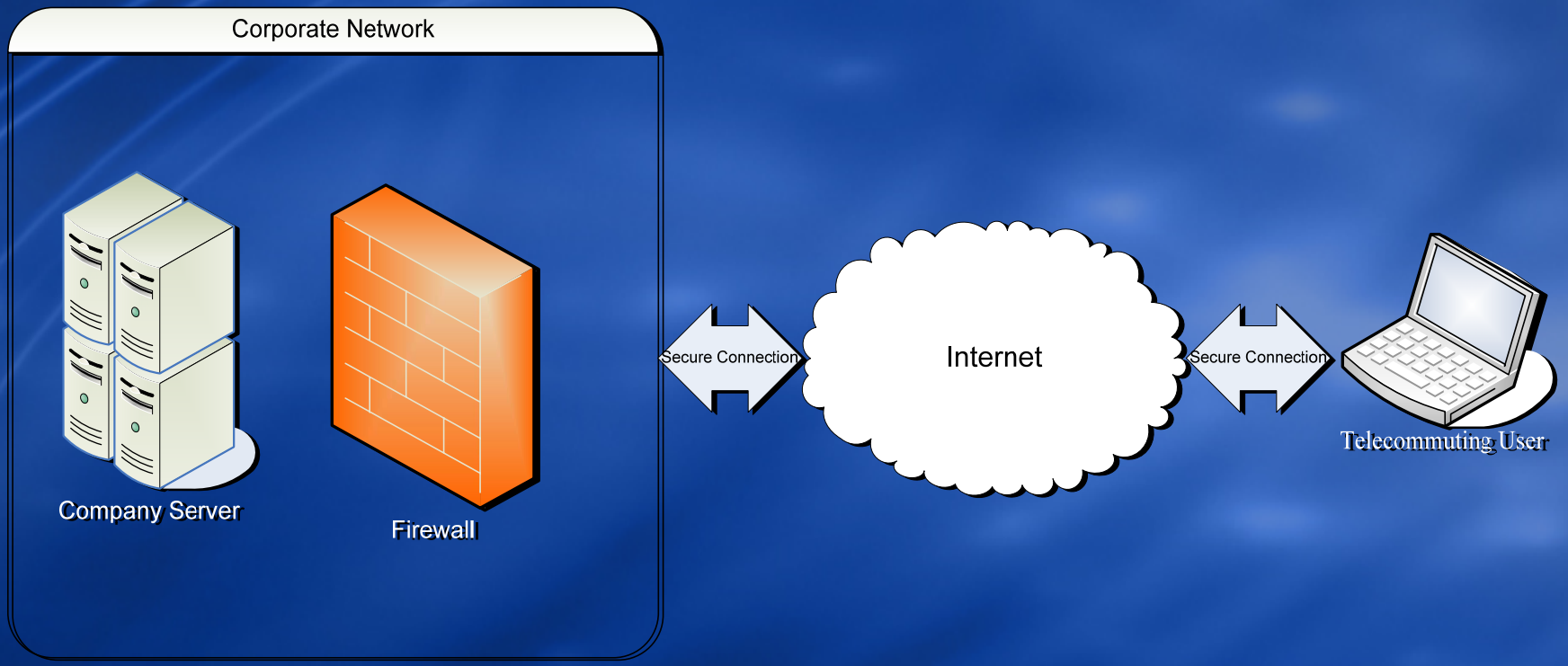
Remote Access Solution

- **VPN (Virtual Private Network)**
  - Types of VPN
    - Web Based VPN: delivers an executable file to the PC and generates a Virtual Private Network
      - Virtual PC/remote PC
    - Client Based VPN: software is installed on the client machine.
- **Dedicated DSL lines**
- **Web mail**

Remote Access Solution

- Components of an Effective VPN:
  - **VPN Client**
  - **VPN Server**
  - **RADIUS Server** (Remote Authentication Dial In User Service)
  - **Firewall**
  - **Encryption or Tunneling Protocol**

Remote Access Solution



Remote Access Monitoring

- **Risks**
  - Unqualified individuals reviewing logs
  - Logs contain too much information and vulnerabilities are overlooked
  - Limited storage space
  - Insufficient Monitoring Process
  - Unauthorized access or intrusions are not detected

Remote Access Monitoring

Solutions / Audit Considerations:

- **Technical User Training Programs**
  - What to look for
  - How often to look
- **Firewall Monitoring**
  - Changes to firewall policy
  - Changes, additions, or deletions of administrative accounts
  - Security violations
- **Firewall Management**
  - Use change management procedures
  - Perform ongoing audits yearly to determine configuration matches the security policy
  - Monitor vendor's security bulletins for security patches
  - Perform vulnerability assessments
  - Periodically backup firewall logs
  - Restrict physical access

Remote Access Monitoring

- **Network Monitoring**
  - Network configurations
  - Analyze usage patterns
  - Detect hacking attempts
  - Detect virus or worm infections

- **Strong network monitoring logs should include:**
  - Synchronized time stamps for each event
  - Sufficient logging level activity to produce detailed events of system activity
  - Sufficient archived logging information

Remote Access Monitoring

- **Database Audit Trails**
  - Logging access to a customer's records (successful or failed)
  - Restricting table level access
  - Fine-grained auditing
  - Automated notifications
  - Classify sensitive data
  - Restrict access to audit trails

Remote Access Monitoring

- **Incident Response Defined:**
  - Incident response is an expedited reaction to an issue or occurrence
- **An Incident Response Plan may minimize the effects caused by a security breach**
  - An incident response plan should be generated, implemented, and tested at least annually
  - Plan should detail the immediate action to be taken, steps for investigating the breach, steps to restore resources, and the process for reporting the incident to proper channels
- **An incident response team should be created to fully investigate potential security breaches**
  - A strong incident response team will receive in-depth training around the incident response plan

Unauthorized Access to Corporate Network

- **Facts**
  - An international gang of cyber criminals hacked into a large/mid-sized bank's records and stole account numbers, created new PINs, fabricated debit cards, then withdrew cash from ATMs (SANS NewsBites, 2008)
  - A computer hacker broke into a large/mid-sized companies database and obtained the names and Social Security numbers of virtually all of the 226,000 Great Falls financial services company's clients (InformationWeek, 2008)

Unauthorized Access to Corporate Network

- **Risks**
  - Damage to company reputation
  - Access to Sensitive Data
    - PII (Personally Identifiable Information)
    - CPNI (Customer Proprietary Network Information)
    - PCI (Payment Card Industry)
  - Infection of viruses
  - Network downtime
  - Unavailable systems and applications

Unauthorized Access to Corporate Network

- **Solutions / Audit Considerations**
  - Two Factor Authentication
    - Something the user **has**
    - Something the user **knows**
    - Something the user **is** or **does**

Unauthorized Access to Corporate Network

- Common Two Factor Authentication Tools
  - Tokens
  - Biometrics

Unauthorized Access to Corporate Network

Security Tokens

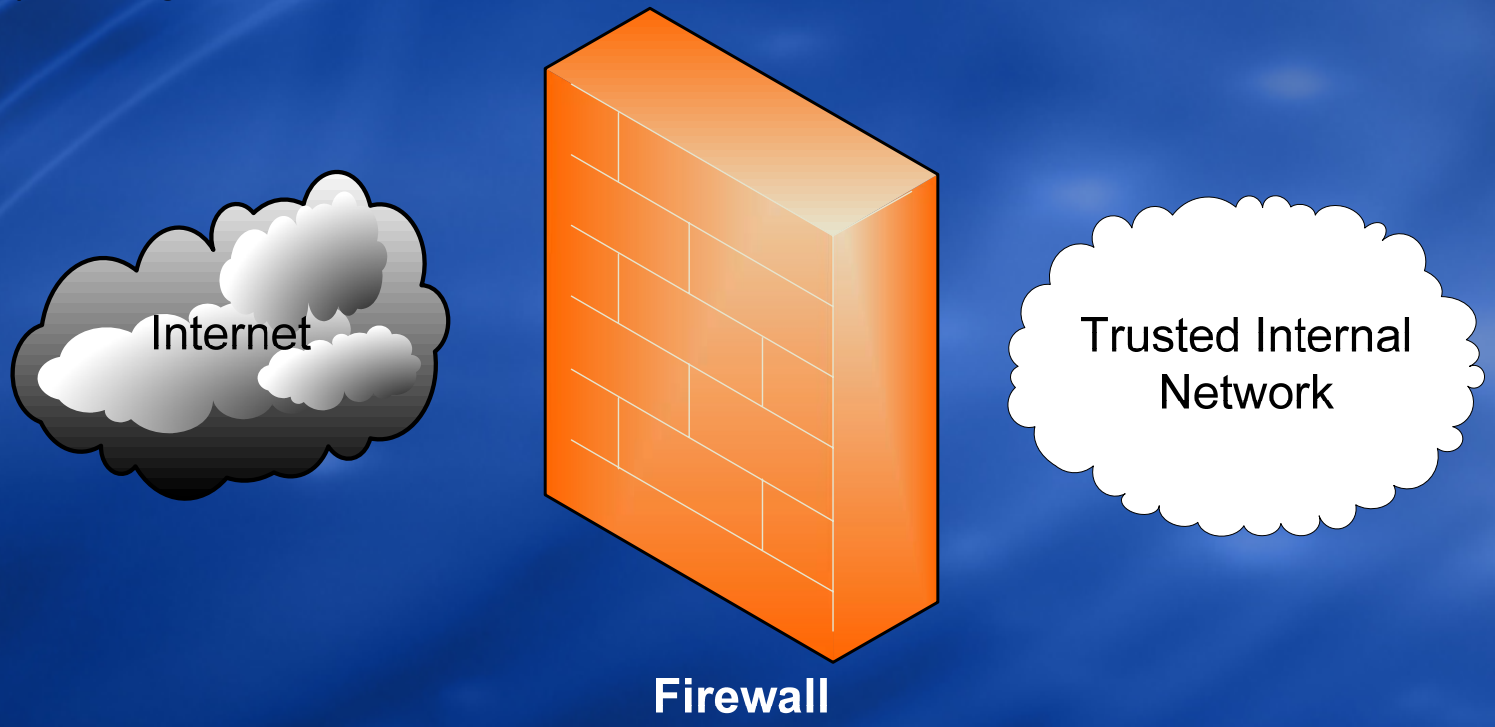
- Security tokens do not require a physical connection to the computer
- The user enters the number displayed on his or her token and a PIN
  - Something you have (**token**) Something you know (**PIN**)

Unauthorized Access to Corporate Network

- **Biometrics**
  - Verification of a user's identity by means of a physical trait
  - Expensive solution
  - Subject to a replay attack

Unauthorized Access to Corporate Network

- **Firewall**
  - Dedicated hardware or software running that inspects network traffic, denying or permitting access based on a set of rules



Unauthorized Access to Corporate Network

- **Types of Firewalls**
  - Network address translation (NAT)
    - Firewall functionality to hide the true address of protected hosts
  - Network level (packet Filters)
    - Inspects packets Stateful & Stateless
  - Proxies
    - Restrict internet access and block content
    - Email
    - Port restrictions

Unauthorized Access to Corporate Network

- **Having a firewall is not an all encompassing security tool**
  - Firewalls cannot protect against
    - Social engineering
    - Disgruntled employees
    - Interception of e-mails
    - Poor physical security
- **Firewalls are a last line of defense**
  - If a hacker is able to bypass the firewall, they will have access to your network, and may have an opportunity to steal data or other sensitive information

Unauthorized Access to Corporate Network

- **An intrusion detection system (IDS) inspects network traffic (inbound and outbound) and identifies patterns that may indicate unauthorized access**

- **What an IDS does**
  - Looks for an attack that has been previously documented
  - Establish a network baseline and investigates outliers
  - Inspects packets across the network
  - Monitors activity on each host (i.e. computer or server)
  - Identifies potential threats
  - Responds to suspicious network activity

Unauthorized Access to Corporate Network

- **Monitoring**
  - Audit Trails
    - Logging access to data or files (successful or failed)
    - Monitoring unusual network activity or personal behavior
  - Software Assistance
    - Helps detect unauthorized access and weaknesses in data protection system

Cost-Benefit Approach to Security

- **Cost-benefit analysis**
  - Identify telecommuting security concerns for your organization
  - Determine what solutions are already in place to mitigate your telecommuting risks and evaluate if additional solutions are needed
  - Determine if the benefits of telecommuting outweigh the costs

Cost-Benefit Approach to Security

- Benefits
  - Reduce office space and lower overhead costs
  - Flexible work schedules and locations – may be able to better serve customers
  - Reduce commuting expenses and time for employees
- Costs to implement
  - Issuing corporate laptops vs. using personally-owned computers
  - Cost of telecommuting software and hardware
    - Personal firewalls, virus protection, VPN, SSH, RSA ids, key fobs
  - Support and maintenance costs for corporate laptops
  - Security training

The Telecommuting Environment

- **Conclusion**
  - Understanding the security concerns in a telecommuting environment increases awareness of the risks and vulnerabilities present, solutions available to mitigate these risks, and reduces the risk of exposing company and client information to unauthorized parties.
  - Telecommuting weaknesses can be addressed through implementation of policies, procedures, education, and technology components

All information provided is of a general nature and not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date is reviewed or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Contact Info

Bryan McGowan
816-802-5856

Clint Newell
816-802-5861