The Insider Threat

Dr. Bruce V. Hartley, CISSP
Privisec, Inc.
August 6, 2003

Session Overview

- Introduction
- The Indispensable Role of the Insider
- Who is the Insider Threat?
- Insider Threat and Lack of Knowledge
- Insider Threat and Social Engineering
- Protecting Your Network Against the Insider Threat
- Conclusions

Before We Get Started

- My Background:
  - In The IT Filed for 22 Years – Security for About 16
  - Currently President and CEO of Privisec, Inc.
  - Previously President and CEO of PoliVec, Inc.
  - Before That, SVP and CTO of Trident Data Systems
  - Academic Credentials:
    - Doctorate in Computer Science From Colorado Technical University, Masters and Bachelors Degrees in Computers as Well…So I'm a Geek…And, Remember: Geek is Sheik!
    - CISSP Since Forever as Well
  - Other Information:
    - Technical Editor for Business Security Advisor Magazine, Formally Internet Security Advisor Magazine
    - Numerous Publications, Conferences, etc.

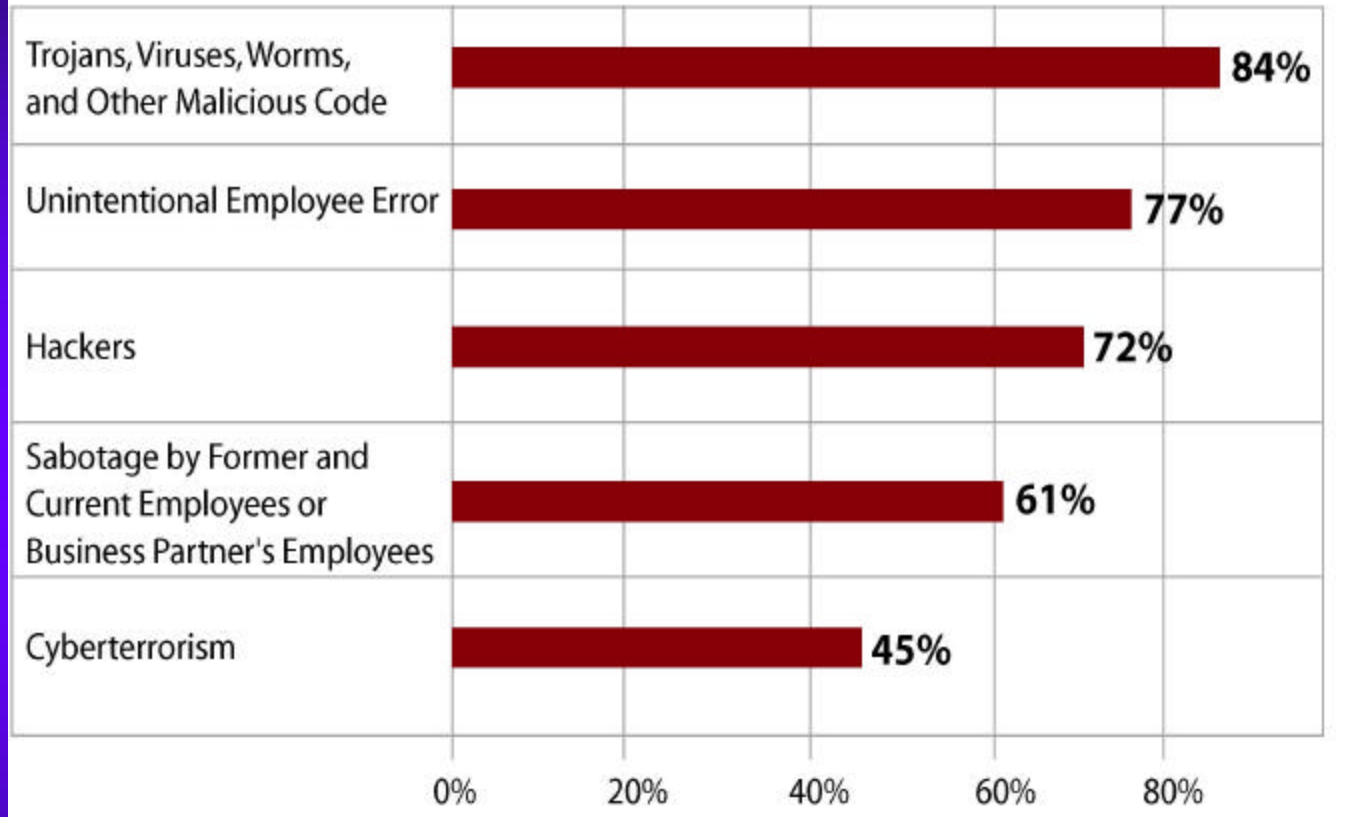
Introduction

- When Thinking About Information Security, the Insider Threat Must be Addressed
- The Insider can be a Threat Against all Three Fundamental Security Principles:
  - Confidentiality, Integrity and Availability
- Insider Problems Exist Today Within our Critical Infrastructure
  - Military, Telecommunications, Energy

Introduction

- Over Half of all Threats Come From Within the Enterprise
  - 70-80% Come From Within According to Pricewaterhouse Coopers and Computer Security Institute
  - Over 51% According to a Meta Group Report, and IDC Survey
  - Statistics may be Skewed Because Many Organizations do not Report Insider Attacks…Worse, Many Went or are Going on Undetected
- The Insider Represents the **Greatest** Threat to Security Because of Their Understanding of the Organizations Business and Systems

What are the Top Five Threats to Enterprise Network Security?



Source: 2003 InfoWorld Security Survey

Introduction

- Due to Their Knowledge and Understanding of Internal Systems and Controls, Insider Attacks are More Likely to be Successful
- The Insider Threat the Greatest Challenge in Securing Your Enterprise Because They are Authorized a Level of Access and Must be Granted a Degree of Trust
- Most Organizations Don’t Want to Consider or Prepare for an Insider Attack as it is “Uncomfortable”

The Indispensable Role of the Insider

- It is Important to Note That the Efforts of "Outside" Groups Can be Aided Significantly by the Assistance of Parties Within the Organization
  - Insiders Have Access to, and Knowledge of, Critical Systems
  - For Certain Secure, Self-Contained Systems, the Insider's Access can Prove Indispensable

The Indispensable Role of the Insider

- The Insider May be “Self” Motivated, Recruited Directly, Recruited Indirectly, Coerced Through Blackmail, or Through Social Engineering
- The Potential Damage an Insider can now Commit has Also Been Increased Within the Last Decade by Two Related Trends:
  - Consolidation
  - Elimination of the “Need to Know” Principle

Who Is The Insider Threat?

- Insiders are Those Individuals who Work for or Have a Relationship With the Target Organization
  - Employees
  - Contractors
  - Business Partners
  - Subcontractors
  - Consultants
  - Customers

Who Is The Insider Threat?

- Many Types of Employees:
  - Disgruntled Employees
  - Paid Informants
  - Compromised or Coerced Employees
  - Former Employees
- Insider Motives Include:
  - Financial
  - Social
  - Political
  - Personal

Case Study 1: The FBI Agent

- Robert Phillip Hanssen, a Career FBI Agent was Charged With Spying for Russia From 1985 to 2001
- Hanssen had Significant IT Experience and Access
- He Allegedly Gave Russian Intelligence Agents Highly Classified Documents About US Intelligence Sources and Electronic Surveillance, in Exchange for an Estimated $1.4M in Cash and Diamonds
- Hanssen Used his Computer Access to the FBI's Electronic Case File System, Which Contains Information About On-Going FBI Investigations, to Check Whether the FBI was Aware of his Activities

Case Study 1: Lessons Learned

- Since Hanssen was an Authorized User, his Queries Didn't Raise Any Suspicion…Obviously Their Log Reduction and Analysis Process Was Less Than Optimal…
- **After** his Arrest, the FBI Correlated his log Activity in the Database With his Espionage Activities
- "In Short, the Trusted Insider Betrayed his Trust Without Detection," FBI Director Louis Freeh Stated at a Press Conference

Case Study 2: Gov't Contractor

- An IT Professional at a Military Base Learned she was Going to be "Downsized"
- She Decided to Encrypt Large Parts of the Organization's Database and Holds it Hostage
- She Contacted the Systems Administrator Responsible for the Database and Offered to Decode the Data for $10,000 in "Severance Pay" With Promise of NO Prosecution
- SA Agrees Before Consulting Proper Authorities

Case Study 2: Lessons Learned

- Prosecutors Reviewing the Case Determined That the Administrator's Deal Precluded Them From Pursuing Charges
- The Insider Walked!
- If Confronted With This Type of Extortion, Be Very Careful About What is Said and/or Done….

Case Study 3: Active Duty

- A Postcard Written by an Enlisted Person was Discovered During the Arrest of Several Members of a Well-Known Hacker Group (by the FBI)
- The Postcard was Written by the Active Duty Person From Their Military Base Where he Served as a Computer Specialist!
- While on Active Duty he Gets Caught Breaking Into Local Phone Systems

Case Study 3: Lessons Learned

- Investigation Reveals the Man to be a Convicted Hacker and Former Member of the Group Who was Offered a Choice Between Prison and Enlistment
- Poor or Missing Background Checks Allowed Individual to Gain Privileged Access to Government Computing Systems
- These Two Examples Demonstrate the Threat Posed by Privileged Users, Such as System Administrators, Programmers, Network Engineers, etc.

Case Study 4: The Subcontractor

- Zhangyi Liu, a Chinese Computer Programmer Working as a Subcontractor for Litton/PRC, Inc., Illegally Accessed Sensitive Air Force Information on Combat Readiness
- He Also Copied Passwords, Which Allowed Users to Create, Modify, and/or Delete Any File on the Network…He Posted These on the Internet!

Case Study 4: Lessons Learned

- This Example Demonstrates the Espionage Threat Posed by Contractors
- The Insider Threat Must be Evaluated and Addressed Throughout the Entire "Business Process"
- In This Case, The Prime Contractor Failed to Ensure the Subcontractor Addressed the Contractual Security Requirements
- Worse, the Gov't Did Not Have an Effective Mechanism to Address This Potential Threat…Allowed the Insider the Access Needed to Compromise the System

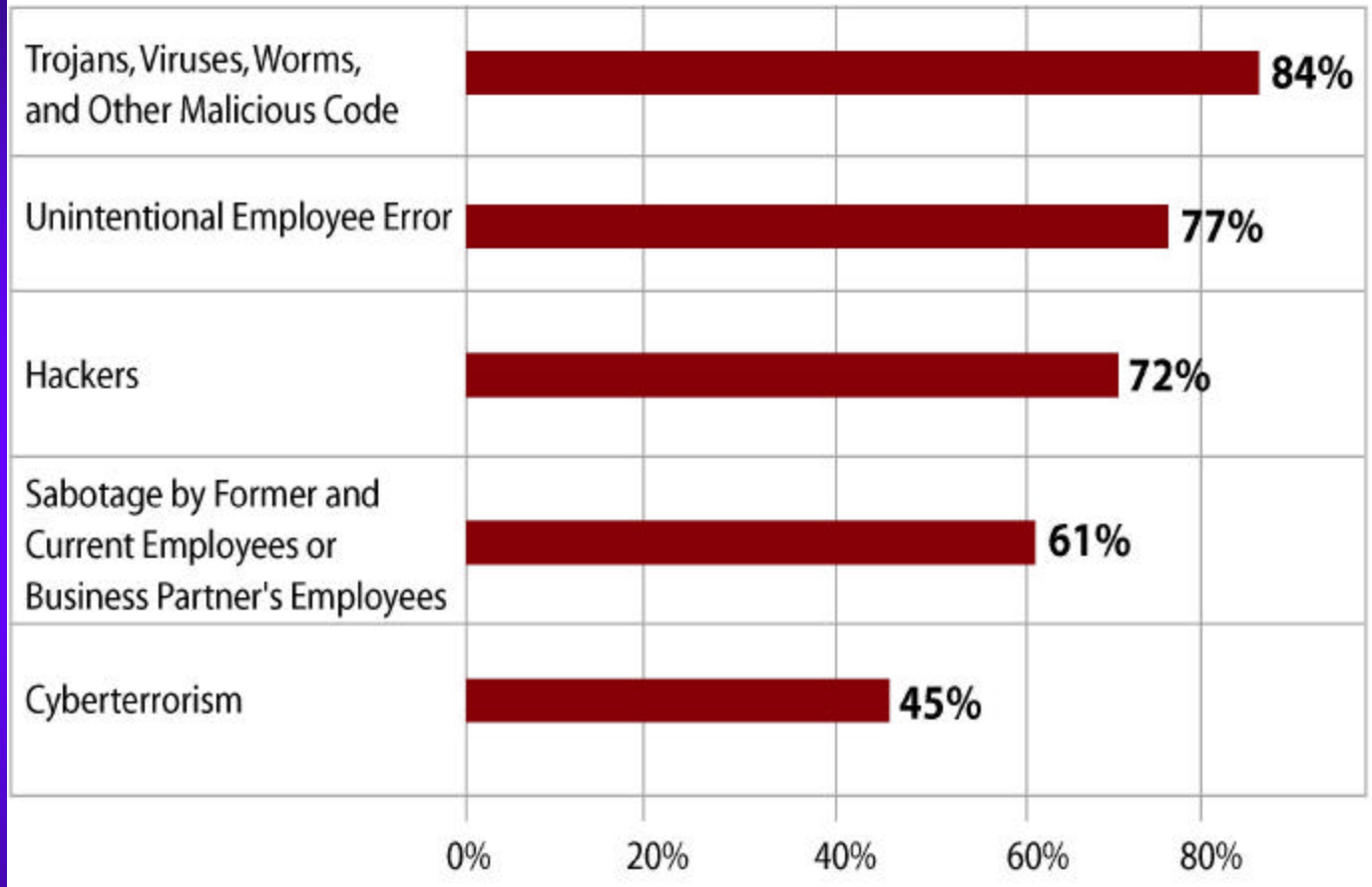
The Insider Threat and the Lack of Knowledge

- Many Network Abuses are a Direct Results of Employees' Lack of Knowledge
- Educating Users is Essential to Computer Security
  - Users Should be Aware of Their Organization's Security Policy and Practices
  - Users Should Understand the Risks of Allowing Other Users Access to Their Accounts, Passwords, Etc.
  - Users Should be Made Aware of the Inherent Risks Associated With Opening Insecure Access on Their Personal Computers or Other Systems
    - Running Web Servers, ftp Servers, etc.
- Enforce the Principle of Least Privilege

The Insider Threat and the Lack of Knowledge

- We Have all Read or Heard That the Insider Threat Accounts for up to 80% of all Security Related Problems
- What is Possibly More Disturbing is That Over Half of all Insider Attacks are Unintentional
- In Many Cases These “Attacks” are Simply Mistakes, Experiments, or Accidents…Not Malicious

What are the Top Five Threats to Enterprise Network Security?



Source: 2003 InfoWorld Security Survey

Case Study 5: The Unintentional Threat

- I was Asked to Investigate a Suspected Denial of Service Attack Against a System Residing on a Military Installation
- After Arriving On-Site, Determined the System Was Running, But That No One Could Access The System
- Basically Had to “Break Into” The System and Then Try to Determine What Had Happened….

Case Study 5…

- After Gaining Access to the System, Found That the /etc/password File was not Available
- Searched the Log Files and Found That the File had Been Accessed by a Privileged User (SA)
- Searched the SA's Home Directory and Found the File
- Turned Out the SA, a Lieutenant, was a Novice Unix SA and Accidentally Mistook the Move Command for Copy Command…Did Not Realize Move Did Not Make a Copy…
- As Folks Logged Off…They Were Locked Out

The Insider Threat and Social Engineering

- Social Engineering is a Low-Tech Method of Cracking Network Security
- Manipulates People Inside the Network Into Providing the Necessary Information to Gain Access
- Some Tactics:
  - Requesting “Help” From a Sympathetic and Unsuspecting User
  - Requesting Information Just Before Quitting Time
  - Masquerading as a Valid User, Manager, Supervisor, Etc.

The Insider Threat and Social Engineering

- Social Engineering can be a Very Effective Means of Attack and Intrusion
- It Plays on the Human Desire to be Helpful and to do the “Right Thing”
- The Defense Against Social Engineering Attacks is an Effective Security Awareness and Training Program
  - Must Inform Users of the These Types of Attacks, to Include Methods and Potential Damages

Protecting Your Network Against Attack

- First and Foremost, Establish a Sound Enterprise Security Policy, Implement it and Enforce it!
- Security Policies Should be Coupled With Platform Specific Implementation Specs
- Educating Users is Also Critical to Developing and Maintaining a Reasonable Security Posture
  - Train Users on the Use of Strong Passwords
  - Ensue That Users Understand how Viruses and Other Programmed Threats Spread and What They Can do to Prevent Such Spreading
  - Make Sure Users are Aware of Social Engineering and how to Handle Such Situations

Protecting Your Network Against Attack

- Additional Protective Measures:
  - Conduct Routine Security Evaluations and Audits
  - Ensure Dial-In Access Control
  - Make Use of Existing Security Features and Mechanisms (Consistently Across Platforms)
  - Eliminate Security Holes – Install Software Updates and Patches
  - Improve Coordination Between Operations Staff and Information Security Staff
  - Improve Skills of the Security Staff
  - Establish Security Awareness and Training Programs
  - Run Backups and Store in a Safe Place (Off-Site)

Protecting Your Network Against Attack

- Additional Protective Measures:
  - Install and Execute Appropriate Anti-Virus Tools (Keep Updated…Engines and Data Files)
  - Routinely Check for and Update Threat Detection Tools as Needed, Especially When New Threats are Discovered
  - Monitor and Manage Firewall Configuration and Rule Sets (Inbound and Outbound)
  - Enforce the Principle of Least Privilege
  - Pre-employment Screening

Protecting Your Network Against Attack

Protecting Your Network Against Attack

- The Biggest Threat to Your Organizations Will Likely Come From the “Trusted Insider”
- Security is Not Mainly About Software, Locks, Biometrics, or Process
- First and Foremost it’s About People and Policies
- Consider a Layered Security Model to Protect Your Organization

A Layered Security Model

- Combination of Administrative and Technical Mechanisms
- Starts With a Commitment to an Information Security Program
  - Dedicate Appropriate Resources and Budget
  - Give Authority to Execute to Company Goals
  - Comprehensive IT Security Policy is a Key Element
  - Must Consider a Process, Not a Project
    - Not Just a GLB Requirement, but a Necessity
      - Need to Account for Changes in Business Model, Services Offered, Technology Updates and New Vulnerabilities

A Layered Security Model

A Layered Security Model

- **Administrative Security**
  - Security Policies, Standards, Guidelines
- **Technical Security Mechanisms**
  - Architectural Security
  - Perimeter/Network Security
  - Host-Based
- **Incident Response and Recovery**
- **Procedural Security**
  - Baseline Protection (Accreditation Process)
- **Security Training and Awareness**

Administrative Security

- Develop and Implement a Consistent Security Policy Across the Enterprise
- Describe The Company's General Security Requirements and Guidelines
  - Roles and Responsibilities
  - Data Classifications and Protection Requirements
  - Enterprise Access Requirements/Process
  - Identification, Authentication, and Auditing
  - Internet Access/Services
  - Dial-Up, Virus Protection….
  - Identify/Describe Use of Standards/Guidelines
- **Make It <u>Official</u> - Make It <u>Mandatory</u>**

Administrative Security

- One of the Biggest Reasons Firms are Vulnerable is Because They Have NOT Established and Implemented a Formal Security Policy
- As a Result, Systems are NOT Consistently Configured and Weaknesses are Common
- Carnegie Mellon University Estimates That 99% of all Reported Intrusions "Result Through Exploitation of Known Vulnerabilities or Configuration Errors, for Which Countermeasures Were Available"

Technical Security -Architecture

- It's Much Easier to Design Security Into an Enterprise Than to Retrofit it
- Evaluate Business Objectives Against the Architecture and Determine What is Required
  - Firewalls and Other Remote Access Controls
  - May Require One or More Demilitarized Zones
  - Intranets and Extranets
  - Web Servers
  - Controlled Dial-In Access
  - VPN-Based Connections
  - Application and Data Segmentation
  - Trust Relationships

Technical Security - Perimeter

- Firewalls
  - Good For Internet and Intranet Applications
  - Many New Features and Services
    - URL/Java Blocking and Screening
    - Virus Protection
    - VPN and Authentication (Data Encryption)
    - WWW Server Load balancing
    - Network Management Integration
    - Secure Dial-In Via Firewall
- Other Secure Remote Access Technologies
  - Virtual Private Networks
  - Secure Remote Access (Dial-In)

Technical Security - Hosts

- Just as Important as Perimeter
- Standard Operating Systems Configurations
  - Password Security, Account Structure, and Audits
  - Trust Relationships (Host Files)
  - Directory and File Permissions
  - Patch Levels and/or Hot Fixes
  - Service Offerings (Like telnet, ftp, etc.)
  - Standardized Virus Protection Software
- Be Consistent, Regardless of Platform or Operating System Type

Incident Handling and Response

- Incident Handling and Response
  - Who Receives and Distributes Security Warnings and Advisories (CERTs, CIAC, Vendor, Other)?
  - What do I do if I Notice a Problem, Like a Break-in Attempt?
  - These are Critical Questions to ask. Remember the Case Studies….
- Incident Handling is Critical
  - The Reason Most Credit Unions are Vulnerable is Because They are NOT Aware of Potential Vulnerabilities or Their Solutions

Procedural Security

- Protecting the Baseline
  - Update Virus Protection Data Files and/or Engines
  - Enforce the Use of Standards and Guidelines
    - Make Compliance Mandatory and Enforce it!
  - Periodic Audits and Controlled Penetrations
- Formal “Accreditation” Process
  - Requires Assessment and Compliance
  - Periodic Re-Certifications Required
  - Re-Certify IF Security Relevant Event Occurs

Security Training And Awareness

- If I Don't Know What to Protect or Why I Should Protect It, I Won't!
  - What Data is Sensitive?
  - What Are The Threats?
- Make Folks Aware of Security Issues and Requirements
- Approach From an Enabling Standpoint, Not a Restrictive Standpoint
- Bottomline: You Cannot Protect a System From Trusted Users - Better to Educate and Train

Conclusions

- A Reasonably Secure Infrastructure is Achievable
  - Must View Security as a Process, Not a Project
  - Embrace Technology and Use it!
  - Be Consistent Throughout the Enterprise
  - Consider the Entire Business Process, Not Just the Transaction Component
- Think About Security From an Enabling Standpoint vs. an Inhibitor
- Be Proactive, Don’t Wait For a Problem to Occur or it Will