Security Policies:
Your First Line of Defense

Dr. Bruce V. Hartley, CISSP

Privisec, Inc.

August 5, 2003

bhartley@privisec.com

719.651.6651

Introduction

- Why Worry About Security?
- What is a Security Policy?
- Why Do I Need One?
- The Security Policy Development Process
- The Contents
- Conclusions and Wrap Up

Before We Get Started

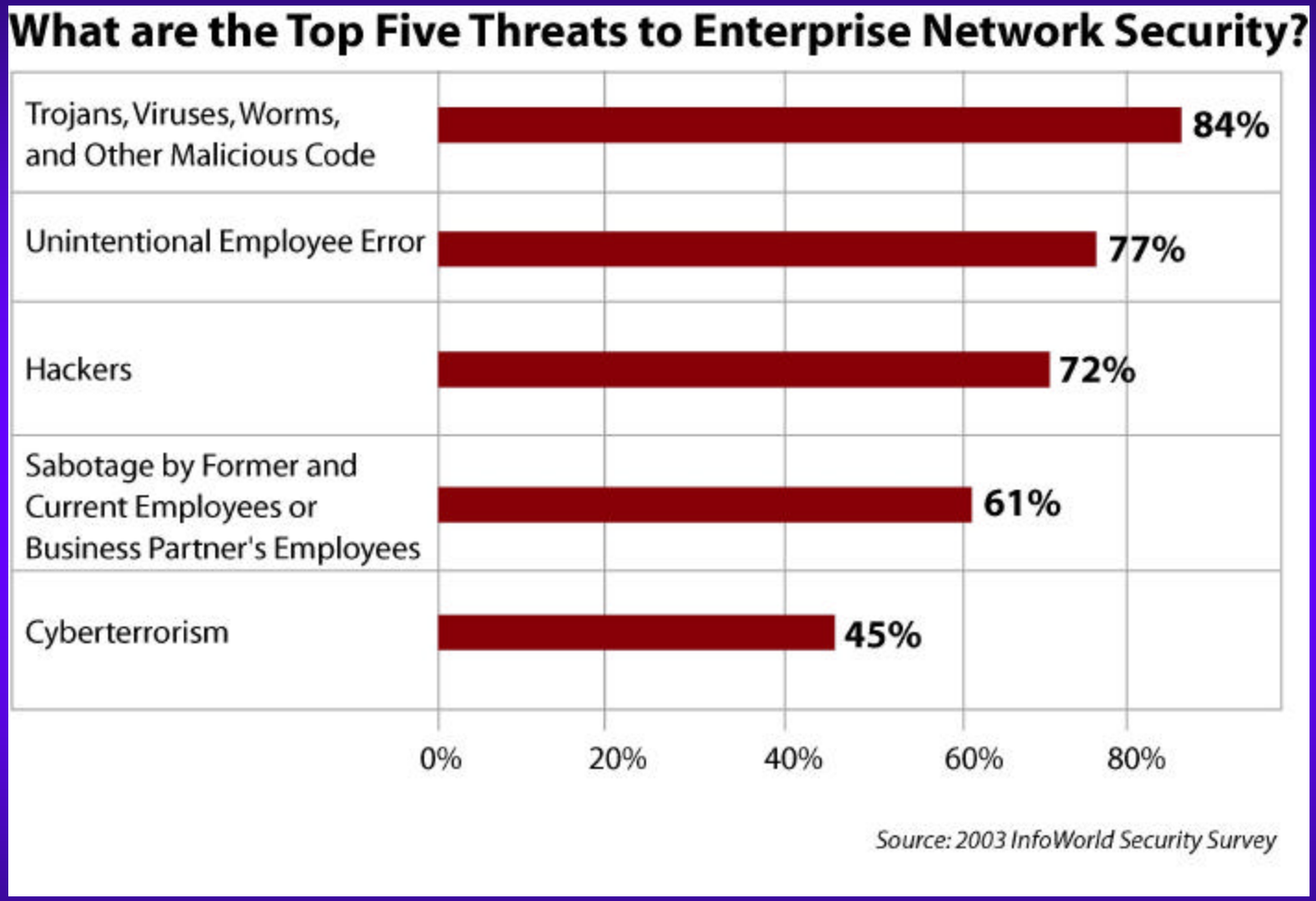
- My Background:
  - In The IT Filed for 22 Years – Security for About 16
  - Currently President and CEO of Privisec, Inc.
  - Previously President and CEO of PoliVec, Inc.
  - Before That, SVP and CTO of Trident Data Systems
  - Academic Credentials:
    - Doctorate in Computer Science From Colorado 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.

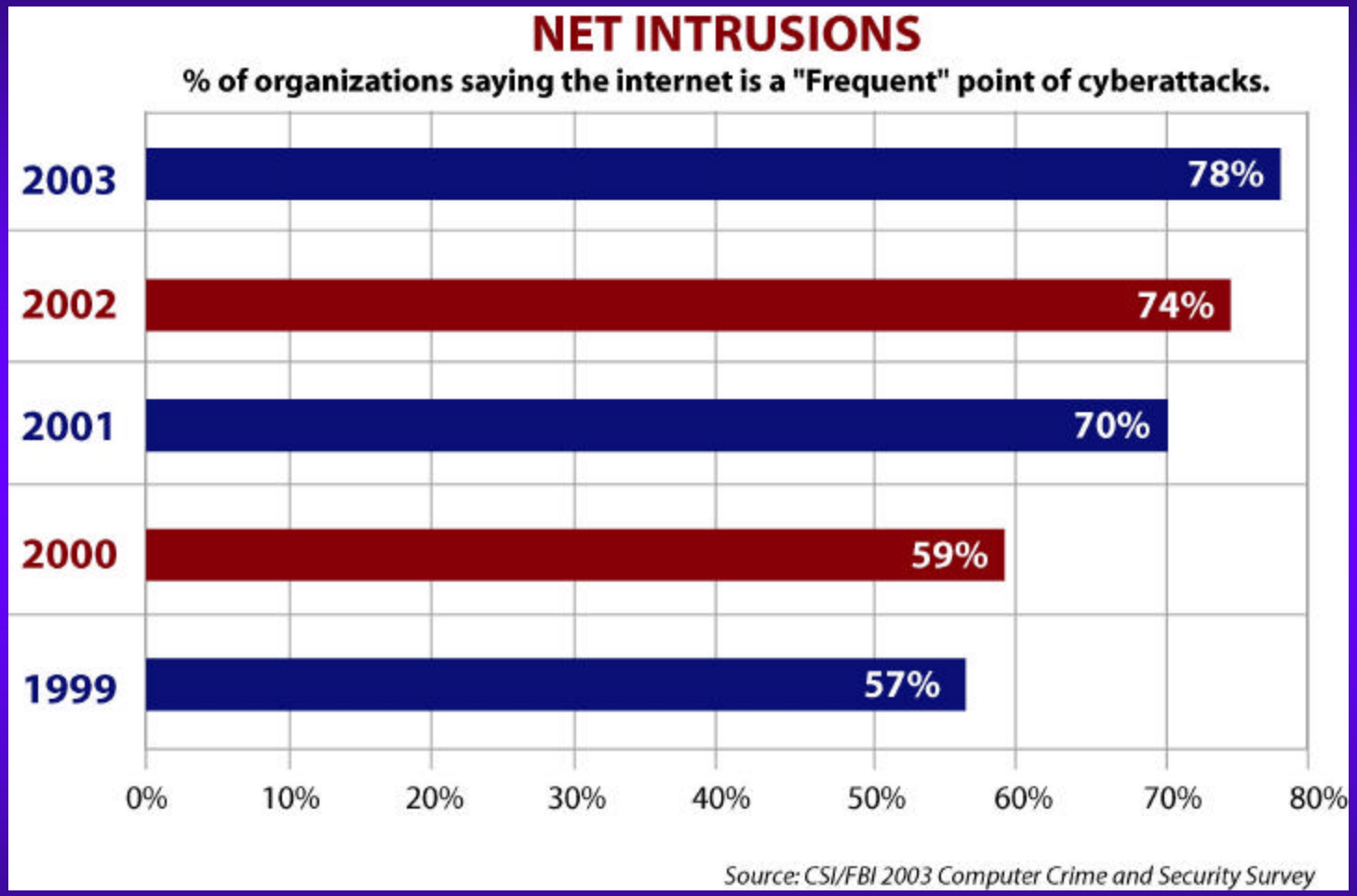
So Why Worry About Security?

- Computer Crime and Abuse is Still a Serious Problem
- Today, Easy to Find Information:
  - Vulnerabilities
  - Exploits
  - Step-by-Step Hacking Guides
- Post Attack Costs are High
- Potential Liability Issues….

Some Recent Statistics

- *An Ernst and Young Security Survey Reported That Over **90%** of Fortune 500 Networks Have Been Hacked*
- *The 2003 CSI/FBI Report States That **95%** of the 530 Respondents Reported Some Form of Unauthorized Computer Use This Year*
- *While Only 251of the Respondents Were Willing to Quantify Financial Losses, They Reported a Total of **$201,797,340** in Financial Losses.*


What are the Top Five Threats to Enterprise Network Security?
Trojans, Viruses, Worms, and Other Malicious Code
84%
Unintentional Employee Error
77%
Hackers
72%
Sabotage by Former and Current Employees or Business Partner's Employees
61%
Cyberterrorism
45%
0%
20%
40%
60%
80%
Source: 2003 InfoWorld Security Survey


NET INTRUSIONS
% of organizations saying the internet is a "Frequent" point of cyberattacks.
2003
78%
2002
74%
2001
70%
2000
59%
1999
57%
0%
10%
20%
30%
40%
50%
60%
70%
80%
Source: CSI/FBI 2003 Computer Crime and Security Survey

Look At The Environment

- Recent Google Search Results:
  - Hacker 12,500,000 Hits
  - Hacker Tools 757,000 Hits
  - Hacker Exploits 103,000 Hits
  - NT Exploits 99,000 Hits
  - Unix Exploits 139,000 Hits
  - Computer Vulnerabilities 403,000 Hits
  - Hacking NT 292,000 Hits
  - Hacking Windows 2000 271,000 Hits
  - Hacking Unix 390,000 Hits
  - Hacking Linux 1,290,000 Hits

The Gramm-Leach-Bliley Act

- Signed Into Law on Nov 12, 1999
- Section 501 of the Act Required Financial Institutions to Perform the Following by July 1, 2001:
  - Insure the Security and Confidentiality of Customer Records and Information
  - Protect Against any Anticipated Threats or Hazards to the Security or Integrity of Such Records
  - Protect Against Unauthorized Access to, or Use of Such Records or Information, Which Could Result in Substantial Harm or Inconvenience to ANY Customer

The Gramm-Leach-Bliley Act

- The Information Security Program Should Include:
  - Security Policies and Procedures
  - Implementation of Those Policies and Procedures
  - Risk and Vulnerability Assessments
    - Remote Penetrations
    - Internal Assessments and Audits
  - Corrective Measures (to Reduce and/or Eliminate Risks)
  - On-Going Evaluations and Processes to Account For Changes and/or Advances in Technology

Some Real-life Case Studies

Recent Penetrations

Recent Penetrations

- Three Examples From the Financial Industry
- All Penetrations 100% Successful
  - Gained “Unauthorized” Privileged Access
  - Access Undetected by Systems Personnel
- All Penetrations Were Preventable – Known Vulnerabilities or Poorly Configured Systems

Financial Institution Union #1

- Gained Access Via Remote Dial-up
- Discovered a Shiva LanRover
- Using Our Default Account Database, Discovered That Account: *root*, Password:<blank> Gave Access to the Server.
- Created a Full Access Account and Set up a PPP Connection Yielding Full Access to the Internal Network

Financial Institution #1

- Also Gained Access Via a Remote Internet Exploit
- Found Web Server Had Both the IIS Vulnerability and the *hk* Vulnerability
  - Gave Full Access to the Server With a Remote Command Prompt
  - Both Vulnerabilities are Publicly Known and Patches are Available From Microsoft
- From This Command Prompt, Access to the Entire Internal Network was Possible

Financial Institution #2

- Gained Access Via a Local Network Exploit
- D-Link Switch Left in Default Configuration
- Default Configuration had SNMP Enabled and, Using a Default Password List, Discovered Full *telnet* Access was Available With Username of "D-Link" and Password of "D-Link"

Financial Institution #2

- Gained Access Via Local Exploit
- Using PoliVec Scanner and Connecting With a Null Session, to get a List of Administrator Accounts
- Gained Administrator Access by Guessing the Password (Password was the Same as Username)
- This Gave Full Access to the NT Domain

Financial Institution #3

- Gained Access Via a Local Network Exploit
- Discovered Several Directories With “Everyone” Granted Full Control Permissions
- Guest Account was Enabled?
- One of the Shared Directories had Sensitive Account Information Including Full Name, Mother’s Maiden Name, SSN, Thumb Print and Other Non-Public Information

Lessons Learned From Penetrations

- Penetrations Were Preventable
- Systems Were Vulnerable for Several Reasons:
  - No Security Policy or Implementation Guidelines to Drive System Configurations
  - IT Staff Not Up to Date on Known Vulnerabilities
  - Poor System Administration/Configuration and Maintenance Practices

Why Do I Need One?

- 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"

The Policy Development Process

- Baseline System Architecture
- Review Existing Security Relevant Policies, Procedures, Guidelines, Regulations, etc.
- Define Protection Requirements
- Develop the Security Policy Document
- Develop Implementation Standards
- Implement the Security Policy!

Baseline System Architecture

- Audit and Document Both Logical and Physical Architecture
- Gather Information on Hardware Platforms, Operating Systems, DMBS, Applications, Network Topology and Connectivity
- This Data Required to Develop a Security Policy That Can Be Integrated and Implemented

Review Security Relevant Policies, Procedures, Regulations

- Make Good Use of Any Existing Work
- Ensure an Understanding of Any Regulatory Requirements
- Identify Gaps in Current Policies and Procedures
- Understand Current Security Posture From an Administrative Point of View

Define Protection Requirements

- Very Similar in Process to a Traditional Risk Assessment Activity
  - Collect Information on Physical, Administrative, and Technical Security
  - Evaluate and Classify Data Types, Storage Locations, and Transfer/Access Requirements
  - Define a Set of Security Rules and Protection Mechanisms

Developing The Security Policy Document

- The Policy Must Consider any Governmental Regulations and/or Guidelines, Local Policies, and
- The Purpose of the Policy is to:
  - Provide Guidance to System Administration Personnel to Help Them Configure and Operate Computer Systems Securely
  - Present a Consistent Stance With Respect to Information Security

Developing The Security Policy Document

- On Presenting a Consistent Stance
  - It is Important to Make sure That the Security Posture at all Access Points to the Network is Enforced in Exactly the Same Manner
- Two Basic Stances:
  - That Which is Not Expressly Permitted is Prohibited; and
  - That Which ids Not Expressly Prohibited is Permitted

Developing The Security Policy Document

- The Two Stances are the Inverse of One Another
- If We Choose the First Stance, We Define What Accesses or Services are Allowed for Users, and All Other Services Are Implicitly Denied
  - This is a Much Better Stance to Base a Security Policy on and the One Recommended

The Contents

- At a Minimum, The Policy Should Consider:
  - Information System Access Approval
  - Identification and Authentication
  - Access Control
  - Security Monitoring and Audit Control
  - Security Training
  - Network Security
  - Physical Security
  - Contingency Planning

Information Systems Access Approval

- Information Access Approval Deals With the Criteria That Must be Met to Obtain Initial Access to a Computer System
- Guidelines are Designed to Effectively Screen Access to the System so That Only Persons Requiring Access are Granted it
- Allows Control and Auditing of Network Users, Which is Important in and of Itself

Identification and Authentication

- I&A is Basically the Process of How a User Identifies Him/Herself, and Then Proves That Identity to a Computer System
- Good I&A is Essential to Good Computer Security and, if Implemented Properly, Can Significantly Reduce Vulnerabilities

Identification and Authentication

- Basically Three Ways to Authenticate:
  - Something You Know – Password/PIN Number, Pass Phrase, etc
  - Something You Have- Smart Card, Token
  - Something You Are – Biometric (Retinal Scan, Finger/Thumb Print, Palm Geometry, etc)
- Can Combine Techniques to Improve Security

Access Control

- Access Control Ensures That Once a User Has Been Authenticated, He/She Can Only Access Files and Services That Are Allowed for That Specific User
- This Mechanism Keeps One User From Reading Another User's Electronic Mail, Files, etc.
- Access Controls for Most Systems is Provided Via Discretionary Access Controls

Access Control

- Access Controls can be set by the Users, on a per User Basis, to Allow Access to any Piece of Data They Own
- Likewise, System Administrators can Control Access of System Files, Operating System Configuration Files, etc.
- Access Controls Should Enforce The Principle of Least Privilege

Security Monitoring and Audit Control

- Auditing and Logging is One of the Most Useful Measures for Detecting and Preventing Unauthorized System Access
- By Default Most Systems Perform Very Little Auditing, But With Some Simple Configuration Changes, Auditing of These Systems Can be Improved Significantly

Security Monitoring and Audit Control

- Once a System is Set up to Audit System Activity, A Plan Should be Created to Make use of the Audit Data
- Auditing Can Create Large Amounts of Data, and Without a Defined Procedure to Analyze the Data, it Will Most Likely Go Unused
- Consider an Automated Audit Reduction Tool to Assist in the Audit Review and Analysis Process
- Note: Many IDS Systems Rely Heavily on Audit Settings and Audit Data

Configuration Management and Testing

- Configuration Management is the Science of Maintaining Control Over the Software, Hardware, User, and Network Configurations of an Enterprise
- Typically the Configuration is Well Known at Installation Time, But as Time Goes On, The Configuration Becomes Loosely Controlled

Configuration Management and Testing

- The Best Type of Configuration Management System Employs Several Components:
  - First, a System for Documentation Must be Defined
  - Second, a Defined Procedure Must be Established to Make Changes to That System
  - Third, All Changes Must be Evaluated Against the Overall Security Posture of the System and, If Allowed, the Change(s) Must be Documented
- Remember, Lack of Good Configuration Management is One of the Main Reasons Systems Get Penetrated

Security Training

- Security Training for Employees That Have Access to Computer Systems is Perhaps the Best Investment With Respect to Total Security
- Studies Have Shown That User Education can Contribute More to the Total Security of a Network Than All Other Countermeasures Combined

Security Training

- Most Security Incidents are Inadvertent Disclosures of Sensitive Information due to a User Understanding the Impact of What He/She was Doing at the Time
- A Good User Education Program can Eliminate These Inadvertent Disclosures and Improve Overall Security Awareness

Network Security

- There are Three Basic Parts to Total Security:
  - Host-Based Security
  - User Education
  - Network Security
- Network Security Deals With Security Mechanisms at the Data Transmission Levels of a Computer Network, and Also at the Perimeter of a Network Where External Connections Reside

Network Security

- For Internal Network Security, it is Important to Have Proper Hardware Configurations, Well Managed Access Points to the Physical Network, and Proper Network Management
- For Perimeter Network Security, a Boundary Needs to be Defined for the Network, and Then Perimeter Security Devices, Such as Firewalls, Need to be Employed to Protect the Network Where it Interfaces to the Outside World

Physical Security

- Physical Security is Still an Important Part of Computer and Network Security
- If an Intruder can Gain Physical Access to the Network, He/She can Usually Gain Unauthorized Access
- Limit Access to System Components Such as Servers, Routers, Firewalls, etc.
- Never Allow Servers to be Used as Workstations

Contingency Planning

- It is Always Important to Have Plans for Disasters Such as Power Outages, Floods, and Other Natural Disasters, as Well as for Malicious Intrusions
- Contingency Plans Should be Implemented With a Minimum of Effort in a Minimum Amount of Time if a Disaster Strikes
- Contingency Plans Should Minimize any Damages or Lack of Service to Users, and it Would be Best if the Transition Were Transparent

On Security Policies

- To be Effective, They Must Have Executive Management Support
- They Must Be Official and They Must be Mandatory
- Unless Implemented, Security Policies Will Only Collect Dust on a Book Shelf

On Implementation Standards

- Once the Security Policy has Been Defines, Develop System Specific Implementation Standards
  - Translates the Policy Into Actual System Configurations
  - Ensures a Consistent Security Posture Throughout the Enterprise, Regardless of Platform
  - Great Configuration Management Tool
  - Helps Demonstrate Regulatory Compliance With Such Things as GLBA!

On Implementation Standards

- Consider Using an Automated Software Tool to Aid in Evaluating and Correcting to a Specific Configuration
  - Microsoft Platforms
    - Microsoft's Baseline Security Analyzer and HFNetChk (Free) – www.microsoft.com
    - PoliVec Scanner – www.polivec.com
  - For Linux and Unix
    - Nessus Scanner (Free) at www.nessus.org

Conclusions

- A Good Security Policy Will Present a Set of Guidelines to be Followed for Operating a Computer System and Also Present a Consistent Stance to all Users
- Once the Security Policy is Defined and Implemented, a Computer System (Enterprise) can Become Reasonably Secure

More Information

- Download my Whitepaper on Security Policy Development at www.privisec.com

My Contact Information

Dr. Bruce V. Hartley, CISSP
President & CEO
Privisec, Inc.

719.651.6651 (Phone)
719.495.8532 (Fax)
bhartley@privisec.com
www.privisec.com