



Pension Benefit Guaranty Corporation

Office of Inspector General

Evaluation Report

**Summary of
Penetration Testing 1999**

December 8, 1999

TABLE OF CONTENTS

I. BACKGROUND

Introduction	3
Scope	3
Work Standards	4

II. APPROACH

Phase I	4
Phase II	5

III. SUMMARY OF FINDINGS

Introduction	6
Strengths	6
Weaknesses	7
Internet Security	7
Dial-In Security	7
Physical Security and Social Engineering Testing	8
Internal Network Security	8

IV. SUMMARY OF RECOMMENDATIONS FOR IMPROVEMENT

8

V. AGENCY COMMENTS AND OIG EVALUATION

TAB I

I. BACKGROUND

INTRODUCTION

PricewaterhouseCoopers conducted a review of network security measures at the Pension Benefit Guaranty Corporation (PBGC). The PricewaterhouseCoopers team conducted network security penetration testing activities focused on components of the PBGC information technology environment in order to identify vulnerabilities and develop recommendations for corrective actions and improvements.

SCOPE

The team used PricewaterhouseCoopers' proprietary diagnostic methodologies and common hacker software tools to identify network vulnerabilities, and compared PBGC information systems security practices with controls observed in industry to identify vulnerabilities and develop recommendations for improvements.

The scope of the penetration testing consisted of:

- ◆ Attempted penetration of PBGC systems from the Internet to determine whether infrastructure and data processing devices are at risk from unauthorized intrusion or abuse via the Internet.
- ◆ Attempted penetration of PBGC systems via telephone modems and dial-in remote access systems to determine if the network is at risk to unauthorized intrusion or abuse via telephone access.
- ◆ Attempted internal penetration of PBGC systems as an insider with physical access to the network infrastructure, and through "social engineering," to determine if PBGC systems are vulnerable to misuse by a malicious insider. The term "social engineering" is used to describe the use of duplicity and social skills to gain sensitive system information.

PricewaterhouseCoopers conducted the testing during the period May, 1999 through July, 1999 at the PBGC office in Washington, DC.

WORK STANDARDS AND LIMITATIONS

PricewaterhouseCoopers conducted this task in accordance with the Standards for Consulting Services established by the American Institute of Certified Public Accountants. Accordingly, PricewaterhouseCoopers provides no opinion or other forms of assurance with respect to the systems reviewed. The procedures were not intended, designed, or performed to identify or detect problems that may result from computer hardware, software, or other automated processes' inability to properly process dates, which includes issues related to Year 2000. The testing provided a view of network security at PBGC at the time of the testing, but due to the nature of information systems security, does not ensure that every possible vulnerability was identified.

II. APPROACH

Phase I: External Network Penetration

◆ Task 1: Internet penetration testing

This task focused on testing the configuration, implementation, and security practices of PBGC's Internet connectivity and access controls. PricewaterhouseCoopers attempted to identify and exploit security vulnerabilities in order to gain unauthorized access into PBGC networks and devices.

Capitalizing on open source and other Internet-based enticement information, the team performed "no-knowledge" outsider penetration testing utilizing a combination of Hacker tools and techniques, commercial software products, and PricewaterhouseCoopers-proprietary methodologies and tools.

Our testing included the following specific actions:

- ✓ Conducting a comprehensive footprint analysis of PBGC Internet connections to identify systems connected to the Internet and services running
- ✓ Testing PBGC Web servers and components of the firewall system using state-of-the-art tools to determine if these components have exploitable configuration weaknesses
- Internet Web site(s) accessible by the public were specifically targeted
- ✓ Reviewing the intrusion detection, monitoring, and effectiveness of incident response capabilities in reaction to penetration tests

◆ Task 2: Dial-in penetration testing

The dial-in testing task focused controlled penetration attacks against known dial-in systems and phone ranges owned by PBGC. The team attempted to penetrate the PBGC network environment by identifying and exploiting dial-in access points. Specific steps were

- ✓ The use of war-dialer software to identify modem paths into the target computer networks within the range of the PBGC telephone exchanges
- ✓ The use of known default accounts, specialized scripts, password guessers, and password cracking software to exploit the remote connections identified in the war dialing
- ✓ Attempts to gain supervisor or root access to the environment followed by attempts to penetrate other hosts that may have a trusted relationship with the host that has been compromised

◆ Task 3: Social engineering testing

At the conclusion of technical external testing, our team used carefully scripted social engineering techniques to attempt to gain additional system information or generate a desired network or user action. The social engineering techniques were scripted jointly by the Office of Inspector General and the PricewaterhouseCoopers team. The objective of the testing was to test PBGC user security awareness and compliance with organizational policies. Common social engineering scenarios include calling the help desk posing as a computer user and asking for the assignment of a new password.

Phase II: Internal penetration

◆ Task 1: Physical penetration testing

The team attempted to gain unauthorized physical access to PBGC systems by circumventing or exploiting weaknesses in the physical security protection of network systems at PBGC. Activities were limited to attempts to enter the building through the main entrance during business hours, locate open office areas or access to data systems or communications closets, and connecting to the network through available network ports.

◆ Task 2: Insider penetration testing

The team performed insider penetration tests in which we attempted to identify vulnerabilities to insider exploitation in order to gain unauthorized access or privileges on critical systems.

and data on the PBGC network. The insider testing assessed PBGC's defenses against malicious individuals with internal access to PBGC facilities and systems. Specific steps performed included:

- ✓ Attempting to gain network access without a valid user account
- ✓ Performing a detailed search and footprint analysis of internal network paths
- ✓ Conducting systematic attempts to gain unauthorized access and privileges via internal and trusted links by exploiting vulnerabilities and network services
- ✓ Analyzing vulnerabilities open to exploitation by attempting to map network topology, increase level of privileges, obtain access to password files, e-mail, and other sensitive data, and gain access to other network segments or subnets
- ✓ Reviewing the intrusion detection and incident response actions

III. SUMMARY OF FINDINGS

◆ Introduction

Penetration testing against PBGC systems revealed that PBGC does not have an effective Information Systems Security Architecture, an enterprise-wide program that defines and enforces security strategy, management, policy, guidelines, standards, and user education.

The absence of an overall architecture of this type leaves PBGC systems vulnerable to malicious external and internal attacks. The level of access gained through the penetration testing gave the team the ability to:

- ✓ Create, delete, or modify PBGC data, including financial and payment information,
- ✓ Access, read, and modify privacy act information on PBGC beneficiaries,
- ✓ Modify PBGC network system configurations,
- ✓ Access PBGC employee network accounts, including administrator accounts on PBGC systems, and
- ✓ Deny service on critical PBGC network systems

◆ Strengths

The penetration testing identified four security measures and control elements employed by PBGC that are considered to be strong. These security and control features are:

- ✓ The Internet firewall configuration blocks unnecessary traffic to the PBGC internal network
- ✓ Security scans of the PBGC Web servers did not identify any significant vulnerabilities
- ✓ Attempts to compromise the Internet mail server were not successful. The team was not able to view electronic mail belonging to PBGC users via the Internet.

- ✓ System security on the production servers was upgraded during our testing, reducing vulnerabilities

◆ Weaknesses

The penetration team was able to obtain extensive unauthorized access to key PBGC systems, including privileges to modify and create data, modify system operating parameters, execute system administration utilities, and create users within production databases and operating systems. Several areas of weakness were exploited, including dial-in, physical, security awareness, and technical configuration vulnerabilities. In addition, the team's activities went undetected and unreported for the duration of the testing.

◆ Internet Security

The team's attempts to penetrate or bypass access controls on the Firewall, web servers, and other Internet systems from the Internet were unsuccessful. The team was not able to gain unauthorized access to PBGC systems via the Internet. At the time of the team's testing, the Internet security controls appeared to protect internal systems from known attacks and unauthorized access via the Internet.

◆ Dial-In Security

Attempts to penetrate PBGC network systems via dial-in access were successful. The team was able to gain access to internal PBGC network systems by exploiting a modem identified through the use of a freely available Hacker war-dialing program. The system was running remote access software that was not password protected, enabling the team to connect to the network as an administrator, and providing a path for our team to access PBGC system files containing sensitive system information.

The team was able to circumvent the access controls on Wide Area Networking (WAN) devices within the PBGC network. The penetration team was able to then use the WAN devices as a conduit into the PBGC network, and identified and exploited PBGC production financial database systems.

The team accessed the PBGC financial systems with a default username and password and then exploited an operating system level vulnerability to gain administrative access to the system. Once administrative access was attained on one system, the team was able to gain access to the other production systems as an administrator. With administrator level access obtained, the penetration team could view and modify data and system files on the production servers.

◆ Physical Security and Social Engineering Testing

After completion of the Internet and dial-in penetration testing efforts, the team conducted physical penetration tests and social engineering tests against PBGC security controls. The testing found PBGC systems vulnerable to unauthorized access and abuse by insiders and outsiders due to physical security and social engineering vulnerabilities.

◆ Internal Network Security

Simulating an unauthorized user with physical access to the PBGC building, the team was able to connect to PBGC systems and gain administrator access, including access to the PBGC electronic mail server. The penetration team was able to masquerade as PBGC users, administer network servers, create and modify data, and access sensitive electronic mail messages. Eventually, the team was able to gain the highest level of access on the production databases. With this level of access, the penetration team could modify, create, and destroy users and data within the production financial databases.

IV. SUMMARY OF RECOMMENDATIONS FOR IMPROVEMENT

PBGC needs to better define and improve its Information Systems Security *Architecture*. This *architecture* is a framework that establishes enterprise-wide strategy and policy, and implements security through technical platform standards, user and administrator security training, monitoring, and response. An effective Information Systems Security architecture is needed if critical PBGC systems, data, and operations are to be protected from unauthorized access, modification, theft, and destruction.

As part of the development and implementation of Information Systems Security Architecture, the following specific actions are recommended:

- ◆ Develop a corrective action plan to enhance the internal network security environment and address the following items:
 - ✓ Adherence to and enforcement of a common password policy for PBGC information systems resources
 - ✓ Evaluation of the PBGC network configuration to determine if traffic between PBGC division networks should be restricted and controlled
 - ✓ Development of technical security implementation guides for information systems within PBGC that instruct and inform administrators of security standards and vulnerabilities associated with their systems
 - ✓ Detailed security reviews of PBGC system configurations
 - ✓ Development of a methodology to periodically check PBGC systems to assess

Pension Benefit Guaranty Corporation

- vulnerabilities within the PBGC network
- ✓ Development of a methodology to ensure that high level access to systems is restricted to necessary users only
- ✓ Development of an Intrusion Management program to detect, repel, respond to, and investigate intrusion attempts into PBGC system
- ✓ The development and implementation of an organizational information security policy that addresses security configurations and standards, policy and procedures, user education, and enforcement of security policies
- ✓ The creation of an Information Systems Security Officer position that reports to the CIO and/or another senior PBGC management official
- ✓ Development of security awareness programs for PBGC information system users and administrators