Editor's Note: The Bank's name and location is fictitious and used for illustration purposes only.

Barnett's Independent Bank & Trust

Blue Water, Texas

Intrusion Risk Assessment Policy

March 25, 2002

Table of Contents

Intrusion Risk Assessment Policy

The information that Barnett's Independent Bank & Trust, Blue Water, Texas (BIBT) has about its customer is a valuable asset. Like all valuable assets, it must be protected against thieves and malicious destruction.

People that would purposely try to steal of destroy the bank's data are referred to as Computer Hackers. Bank's are an attractive target for Hackers, and management at BIBT realizes this.

Research has shown that 70% of Hacker break-ins are done by a company's own employees. Accordingly, it is impossible for BIBT to eliminate the risk that someone will gain unauthorized access to one (or more) of the bank's systems. However, management can implement policies and procedures that minimize the risk of loss.

This policy documents the various computer systems that the bank uses, and the measures taken to reduce the risk of a Hacker break-in.

1. Core Banking System.

Criticality of system to bank operations: High

Accessible to Hackers: Yes, via the network router and local area network.

Measures taken to reduce risk of penetration:

1) Installation of an Internet firewall.
2) Restricted access to the mainframe command line.
3) Restricted access to upload and download programs.
4) Restricted access to system utility programs.
5) System modem in kept off-line when it's not in use.
6) Assignment of unique user-IDs and confidential passwords.
7) Prompt canceling of inactive system sessions.
8) Requirement to work with well known, well capitalized vendors.

Likelihood of a Hacker break-in: Low

Potential loss to bank: Minimal, because of compensating measures.

Actions to be taken in the event of a break-in:

1) Disconnect Internet connection from router.
2) Disconnect phone line from modem.
3) Disconnect mainframe from router. (This will disable all terminals, except for the main console.)
4) Contact the FBI, the local police, and the primary Regulator.

5) Contact vendor for primary system.

2. Fed Line Operations

Criticality of system to bank operations: Medium

Accessible to Hackers: Yes, if he has access to the system server.

Measures taken to reduce risk of penetration:

1) Use of Fed Line System security controls.
2) Separation of duties.

Likelihood of a Hacker break-in: Low

Potential loss to bank: Minimal, because of compensating measures.

Actions to be taken in the event of a break-in:

1) Contact Fed Dallas.
2) Contact the FBI, the local police, and the primary Regulator.

3. Check Imaging and POD Operations

Criticality of system to bank operations: Medium

Accessible to Hackers: Yes, if he has access to the system server.

Measures taken to reduce risk of penetration:

1) Use of system security controls.
2) Separation of duties.

Likelihood of a Hacker break-in: Low

Potential loss to bank: Minimal, because of compensating measures.

Actions in the event of a break-in:

1) Contact the vendor
2) Contact the FBI, the local police, and the primary Regulator.

4. Internet Banking System

Criticality of system to bank operations: Medium

Accessible to Hackers: Yes, via the network router.

Measures taken to reduce risk of penetration:

1) The web server is kept off-site, and, managed by a professional Internet Service Provider (ISP) vendor.
2) Contract with the ISP vendor stipulates that it will have an annual third party SAS 70 audit.
3) Contract with vendor also stipulates that it will have annual third party penetration tests.
4) All audit and penetration test reports for the vendor are reviewed by BIBT management
5) All regulatory reports for the vendor are reviewed by BIBT management
6) The vendor must respond in writing to any critical weaknesses noted by auditor and examiners.
7) Vendors financial condition is monitored on at least an annual basis. More frequent monitoring will occur if the vendor starts having financial trouble.
8) Users of the system are required to use an Internet browser that has a minimum of 32-bit encryption.
9) New users of the system must authenticate their identity, prior to being allowed to enroll for the service.
10) System users that require customer service (e.g., password resetting, user-ID resetting, etc.) must authenticate their identity, prior to the service being rendered.

Likelihood of a Hacker break-in: Low

Potential loss to bank: Minimal, because of compensating measures.

Actions to be taken in the event of a break-in:

1) Contact vendor for primary system.
2) Contact the FBI, the local police, and the primary Regulator

5. Local Area Network

Criticality of system to bank operations: Medium

Accessible to Hackers: Yes, via the router, e-mail, and local area network.

Measures taken to reduce risk of penetration:

1) Installation of an Internet firewall.
2) Assignment of unique user-IDs and confidential passwords for the network.
3) Installation of a virus detection system, with an auto-update feature that automatically interacts with the vendor's web site.

4) Assignment of private directories.
5) Careful control of shared directories.
6) Restricted use of Admin rights.

Likelihood of a Hacker break-in: Low

Potential loss to bank: Minimal, because of compensating measures.

Actions to be taken in the event of a break-in:

1) Contact network support company.
2) Contact the FBI, the local police, and the primary Regulator.

6. Internet & E-mail Operations

Criticality of system to bank operations: Low

Accessible to Hackers: Yes, via the ISP, network router & e-mail.

Measures taken to reduce risk of penetration:

1) Installation of an Internet firewall.
2) Installation of a virus detection system, with an auto-update feature that automatically interacts with the vendor's web site.

Likelihood of a Hacker break-in: Low

Potential loss to bank: Minimal, because of compensating measures.

Actions to be taken in the event of a break-in:

1) Contact ISP.
2) Contact network support company.
3) Contact the FBI, the local police, and the primary Regulator.

7. ATM System

Criticality of system to bank operations: Low

Accessible to Hackers: Yes, if he has access to the system server.

Measures taken to reduce risk of penetration:

1) Use of system security controls.
2) Separation of duties.

Likelihood of a Hacker break-in: Low

Potential loss to bank: Minimal, because of compensating measures.

Actions to be taken in the event of a break-in:

1) Contact the vendor
2) Contact the FBI, the local police, and the primary Regulator.

8. Debit Card System

Criticality of system to bank operations: Low

Accessible to Hackers: Yes, if he has access to the system server.

Measures taken to reduce risk of penetration:

1) Use of system security controls.
2) Separation of duties.

Likelihood of a Hacker break-in: Low

Potential loss to bank: Minimal, because of compensating measures.

Actions to be taken in the event of a break-in:

1) Contact the vendor
2) Contact the FBI, the local police, and the primary Regulator.

9. Telephone Banking System

Criticality of system to bank operations: Low

Accessible to Hackers: Yes, if he has access to the system server.

Measures taken to reduce risk of penetration:

1) Use of system security controls.

Likelihood of a Hacker break-in: Low

Potential loss to bank: Minimal, because of compensating measures.

Actions to be taken in the event of a break-in:
1) Contact the vendor
2) Contact the FBI, the local police, and the primary Regulator.

10. Teller System

Criticality of system to bank operations: Low

Accessible to Hackers: Yes, if he has access to the system server.

Measures taken to reduce risk of penetration:

1) Use of system security controls.

Likelihood of a Hacker break-in: Low

Potential loss to bank: Minimal, because of compensating measures.

Actions to be taken in the event of a break-in:

1) Contact the vendor
2) Contact the FBI, the local police, and the primary Regulator.

11. New Deposit and New Loan Systems

Criticality of system to bank operations: Low

Accessible to Hackers: Yes, if he has access to the system server.

Measures taken to reduce risk of penetration:

1) Use of system security controls.
2) Separation of duties.

Likelihood of a Hacker break-in: Low

Potential loss to bank: Minimal, because of compensating measures.

Actions to be taken in the event of a break-in:

1) Contact the vendor
2) Contact the FBI, the local police, and the primary Regulator.

12. Check ordering System

Criticality of system to bank operations: Low

Accessible to Hackers: Yes, if he has access to the workstation PC or LAN.

Measures taken to reduce risk of penetration:

1) Use of system security controls.
2) Deactivate the auto-answer feature on the PC modem.

Likelihood of a Hacker break-in: Low

Potential loss to bank: Minimal, because of compensating measures.

Actions to be taken in the event of a break-in:

1) Disconnect the phone line to the modem.
2) Contact the vendor.
3) Contact the FBI, the local police, and the primary Regulator.

13. Workstation PCs

Criticality of system to bank operations: Low

Accessible to Hackers: Yes, if he has access to the workstation units or LAN.

Measures taken to reduce risk of penetration:

1) Limit the use of dial-up modems.
2) Activate the BIOS passwords
3) Activate the screensaver passwords.

Likelihood of a Hacker break-in: Low

Potential loss to bank: Minimal, because of compensating measures.

Actions to be taken in the event of a break-in:

1) Disconnect the phone line to the modem.
2) Contact the FBI, the local police, and the primary Regulator.