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
Information Security Policy
March 25, 2002
Table of Contents

Security Objectives ............................................................................................................. 1

Working with Independent Service Providers ................................................................. 1

Threats to Security Controls ............................................................................................. 2

Threat #1: Confidential customer information could be stolen. ..................................... 2

Threat #2: A computer hacker could maliciously destroy customer data. .................. 3

Threat #3: Unauthorized transactions could be posted to a customer’s account. ...... 3

Threat #4: Password integrity could be compromised. .................................................. 4

Threat #5: Customer data could be lost due to a catastrophic event. ......................... 5

Reporting Attempted or Actual Breaches of Security ....................................................... 5

Review and Revisions of Security Program .................................................................... 5
Information Security Policy

Customer information is a valuable asset. People trust banks to keep their personal financial information confidential. Banks are required by law to have policies and procedures that protect against accidental, or intentional, misuse of the information.

The board of directors at Barnett’s Independent Bank & Trust, Blue Water, Texas (BIBT) is committed to preserving and protecting customers’ information. To that end the directorate developed this Information Security Policy.

Security Objectives

The Information Security Program at BIBT is designed to ensure that the following security objectives are met:

1. Customer information will be kept secure and confidential. The bank will implement a series of controls that help safeguard information from unauthorized viewing by non-bank personnel. Also, information about our customers will not be sold, exchanged, or given away without their prior written consent.

2. Known and anticipated threats to BIBT’s Security Program will be documented, along with the measures taken to minimize the likelihood of the threats occurring.

3. Management will be proactive in searching for new threats to the bank’s Security Program. Specifically, it will attend seminars and training classes on how to protect customer information. The bank will also have an annual review of its information technology operations by a qualified third party.

Working with Independent Service Providers

BIBT will periodically work with Independent Service Providers. Most notably, the bank will hire third parties to perform financial audits, information technology (IT) examinations, Community Reinvestment Act (CRA) examinations, and loan reviews. Also, the bank will purchase data processing services from various companies; send checks, wire transfers, and ACH transactions to non-affiliated banks; and, work with regional credit bureaus.

In all instances, unless the Independent Service Provider is a government entity (such as the Federal Reserve), the bank will ask for a written statement from the Service Provider where they attest to having a Security Program that meets the security objectives outlined in this policy. If the Service Provider refuses to provide such a statement, the service contract will be abrogated. (Note: contracts currently enforce are excluded from this requirement, unless the contract expires subsequent to July 1, 2003. Contract
expiring subsequent to this date will be amended to stipulate that suitable security procedures will be maintained.

**Threats to Security Controls**

This portion of the policy identifies potential threats to BIBT’s Security Controls, and what management has done to address them.

**Threat #1:  Confidential customer information could be stolen.**

**Potential damage to BIBT & Customers:**

The theft of confidential information could result in BIBT’s customers being victims of identity theft.

**Measures taken to control threat:**

1. All discarded reports and other confidential information is securely stored until it can be destroyed.

2. Employees will secure all reports and documents in their possession, prior to leaving for the day.

3. The ability to download data from the bank’s system is restricted to those few employees that have a need to do so.

4. Access to the mainframe computer is restricted through the use of system passwords and an automatic canceling of idle system sessions.

5. Access to personal computers is restricted through the use of screensaver passwords and basic input/output system (BIOS) passwords.

6. Personal computers and electronic media that are removed from service are reformatted prior to disposal.

7. A criminal background check is ran on all potential new employees, prior to them being hired.

**Likelihood that threat will be realized:** Minimal, because of the controls that BIBT has in place.

**Additional measures needed at this time:** None.
Threat #2: A computer hacker could maliciously destroy customer data.

Potential damage to BIBT & Customers:

The purposeful destruction of customer data could result in BIBT being unable to charge customers for withdrawals, or credit customers for deposits.

Measures taken to control threat:

1. To protect against external hackers, the bank has installed an Internet firewall and virus detection software.
2. The virus detection software is updated as often as daily, via an auto-update feature that interacts with the vendor’s web site.
3. The bank’s IT manager checks each month, to see if there has been an update for the firewall software. All new updates are installed.
4. To protect against internal hackers, the bank limits access to “Command Line Instructions” for the mainframe computer.
5. All data files for the primary bank systems are backed-up daily and stored off-site.

Likelihood that threat will be realized: Minimal, because of the controls that BIBT has in place.

Additional measures needed at this time: None.

Threat #3: Unauthorized transactions could be posted to a customer’s account.

Potential damage to BIBT & Customers:

The bank could suffer a material loss, in the event an employee embezzles funds by making withdrawals from other people’s accounts.

1. The security system that’s incorporated in the primary banking system is used to enforce a separation of duties.
2. All on-line posted transactions are independently reviewed, the day after they occur.
3. Access to dormant accounts is strictly limited.
4. The ability to change name and address information is strictly limited.

5. There is an independent review of newly issued and modified ATM and debit cards.

6. Wire transfer transactions are executed under dual control.

7. In most instances, customers must come to the bank to initiate a wire transfer transactions. The few transactions that are allowed to be remotely initiated are confirmed with a recorded call-back.

8. ACH files must be delivered to the bank electronically, or, delivered by someone who has transaction authority for the account.

   Likelihood that threat will be realized: Minimal, because of the controls that BIBT has in place.

   Additional measures needed at this time: None.

**Threat # 4: Password integrity could be compromised.**

Potential damage to BIBT & Customers:

   Someone could post unauthorized transactions, by using a coworkers user-ID and password.

Measures taken to control threat:

1. All employees are assigned individual user-IDs.

2. All employees select their own system passwords.

3. The system forces employees to select passwords that are hard to guess.

4. The system forces employees to change their passwords every 45 days.

5. The system prohibits employees from repeatedly using the same password.

6. Management is aware of the risk associated with “keyboard capture programs”. All PCs that suddenly begin start to malfunction will be checked for such programs.
Likelihood that threat will be realized: Minimal, because of the controls that BIBT has in place.

Additional measures needed at this time: None.

**Threat # 5: Customer data could be lost due to a catastrophic event.**

Potential damage to BIBT & Customers:

The destruction of customer data as a result of fire, tornados, or other catastrophic event could result in a loss of customer records.

Measures taken to control threat:

1. The master files are backed-up each night, and the backup files are stored off-site.

2. BIBT has two (2) off-site methods for restoring the system.

3. The off-site storage location is far enough from the bank to minimize the risk that one catastrophe will destroy both the primary and backup data files.

4. BIBT uses a high-quality brand of tape media, and replaces the tapes once a year.

Likelihood that threat will be realized: Minimal, because of the controls that BIBT has in place.

Additional measures needed at this time: None.

**Reporting Attempted or Actual Breaches of Security**

All breaches and attempted breaches of the bank’s security controls will be reviewed to the appropriate legal authorities, via a Suspicious Activity Report.

All breaches and attempted breaches will also be reported to directorate, by the bank’s Security Officer.

**Review and Revisions of Security Program**

The bank’s chief operating officer (COO) is responsible for maintaining this policy and ensuring compliance. The Security Policy will be reviewed and revised annually by the board of directors, or its appointed committee.