NETWORK REMOTE ACCESS
RISK MANAGEMENT

Keylogger and other types of malicious software can allow unauthorized users access to a Bank employee’s Bank network account. See the below news story. It discusses how an unnamed financial firm employee’s PC infected with a keylogger program allowed hackers to take over her PC and access the company’s network. One of the most popular items that can be cheaply purchased from Amazon.com is a keylogger hardware device that stores a user’s key strokes as they are typed; the device is later retrieved by the criminal. It is typically plugged into the cord going from the keyboard to a desktop PC and no anti-virus software will detect this since it isn’t software.

**Bank users of GoToMyPC or other remote connection systems could expose Capital Bank to this risk.**

Once someone is authenticated to come into the Bank’s network using legitimate user ID’s and passwords, they are in. The Bank must rely upon employees to follow safe practices to try our best to prevent an intrusion in the first place. If the PC used to access the Bank’s network, whether personal at home or a computer used at a public place such as a library, internet café, etc., is infected with a malicious keylogger program or has one of these keylogger devices installed, the recipient of the log on key stroke information will see all key strokes used to log onto the Bank’s network via GoToMyPC. S/He can exploit the Bank’s and its customers’ confidential information and play all sorts of terrible havoc with the Bank’s systems before being discovered.

In addition to the network and user policies the Bank has in place to limit the potential for mischief, Bank employees granted privileges for remote access are expected to –

- Be especially aware of these risks;
- Keep personal or Bank owned laptops used to access the Bank’s network up to date with security and software updates and patches and
- Take reasonable and responsible actions to lessen the possibility of unauthorized access to the Bank’s network. (“Guidelines” below.)

**Guidelines**

1. Use your own PC or a Bank laptop to access the Bank’s network via GoToMyPC – never use a public computer to log on to the Bank via GoToMyPC.
   a. If you have a Bank issued laptop, it must be brought in to the Bank regularly to plug into our network and have the latest software updates and anti-virus protection updates installed.
2. Employees who are granted remote access privileges are required to assure their own PC is up to date with anti-virus/malware software to prevent keyloggers and other malware from being installed.
   a. If you need assistance with what anti-virus software is advisable, contact the Bank’s IT Manager for assistance.
3. Be very careful what you click on in emails you receive, even from people you know. Many malware programs are so sophisticated that you won’t even know they have installed themselves.
4. Don’t log on as a local administrator for regular browsing and email reading at home. Software programs need local admin access to install themselves. If you are logged on as “just” a user, that will help provide some protection and will let you do what you need to do the majority of the time. Only use the local admin. user when you need to install a program on your PC.
5. Re-read the Bank’s Remote Access Policy, attached.
Phishers Used Facebook to Penetrate Financial Firm's Computer System
March 4, 2010
Phishers used Facebook to burrow their way into the network of a large US financial company last year. The attackers took control of one employee's Facebook account and using information culled from that individual's friends' profiles, sent what appeared to be personal messages to several other company employees about pictures taken at a company picnic. The phishers learned of the picnic through postings on the hijacked account. When one of the other employees received a message asking her to click on a link that would allow her to view the pictures, her computer became infected with keystroke logging malware. When that employee logged in to a VPN account to access the company network, the attackers were able to capture the necessary information to gain access to that network. The intruders managed to get deeper into the network and take control of two servers before they were detected.

I acknowledge that I have read and agree to abide by the guidelines above and the Bank’s Remote Access Policy attached to obtain and maintain my remote access privileges to the Bank’s network.

Date:______________________________

Signed:____________________________________

Print Name:__________________________________
1.0 Purpose
The purpose of this policy is to define standards for connecting to the Bank’s network from any host. These standards are designed to minimize the potential exposure to the Bank from damages which may result from unauthorized use of the Bank’s resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Bank internal systems, etc.

2.0 Scope
This policy applies to all Bank employees, contractors, vendors and agents with a Bank owned or personally-owned computer or workstation used to connect to the Bank’s network via a means outside of the Bank’s wired LAN and/or WAN network. This policy applies to remote access connections (for example home offices) used to do work on behalf of the Bank, including reading or sending email and viewing internet or intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

3.0 Policy

3.1 General
1. It is the responsibility of Bank employees, contractors, vendors and agents with remote access privileges to the Bank’s corporate network to ensure that their remote access connection is given the same consideration as the user’s on-site connection to the Bank.

2. For those employees who have Remote Access, they acknowledge receipt and understanding of the requirements set out in the Computer Technology & Internet Acceptable Use Policy. All of the requirements, prohibitions and provisions of that policy are applicable when an employee accesses the Bank’s internal network from a remote location.

3.2 Requirements
1. Secure remote access must be strictly controlled. Control will be enforced via password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Computer Technology & Internet Acceptable Use Policy.

2. At no time should any The Bank employee provide their Bank network login or email password to anyone, not even family members.

3. The Bank employees and contractors with remote access privileges must ensure that their Bank-owned or personal computer or workstation, which is remotely connected to
The Bank's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

4. The Bank employees and contractors with remote access privileges to the Bank's corporate network must not use non-Bank email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct Bank business to ensure that official business is never confused with personal business.

5. Bank employees may not download and save to non-bank owned computers any data from the Bank’s network.

6. If any data are printed from the Bank’s network at a remote location, the employee shall return the printed data to the Bank for proper destruction or shall securely destroy (shred) the printed documents through a paper shredder.

7. Routers for dedicated ISDN lines configured for access to the Bank network must meet minimum authentication requirements of CHAP.

8. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.

9. Frame Relay must meet minimum authentication requirements of DLCI standards.

10. Non-standard hardware configurations must be approved by the IT Manager as well as security configurations for access to hardware.

11. PC's connected to The Bank internal networks via remote access technologies must use the most up-to-date anti-virus, anti-spam, anti-malware software. Third party vendors must comply with requirements as stated in their respective vendor agreement.

12. Personal equipment that is used to connect to The Bank's networks must meet the requirements of The Bank-owned equipment for remote access.

13. Organizations or individuals who wish to implement non-standard Remote Access solutions to the Bank’s production network must obtain prior approval from the IT Manager.

14. All parties (employees & contractors), must have approval from Management to gain Remote Access Privileges

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions
1. Cable Modem - Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.

2. CHAP - Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function.
3. DLCI - Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.

4. Dial-in Modem - A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.

5. Dual Homing - Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Corporate network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a Bank-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into The Bank and an ISP, depending on packet destination.

6. DSL - Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).

7. Frame Relay - A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.

8. ISDN - There are two flavors of Integrated Services Digital Network or ISDN: BRI and PRI. Basic Rate Interface (BRI) is intended for the home and small enterprise, and the Primary Rate Interface (PRI), for larger users. Both rates include a number of B-channels and a D-channel. Each B-channel carries data, voice, and other services. The D-channel carries control and signaling information.

9. Remote Access - Any access to the Bank's corporate network through a non-Bank controlled network, device, or medium.

10. Split-tunneling - Simultaneous direct access to a non-The Bank network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into The Bank's corporate network via a VPN tunnel.

11. VPN - Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.