SIMPLY PROTECTING DATA

by Steve Brown

There are basically two types of people - those who like technology and those who could do without it. If you have been a reader of this publication for any period, you know we fall squarely into the first camp. We see technology as a significant enabler. Whatever group you are in, however, we readily admit the biggest problem we have when it comes to technology is keeping up with what is relevant. So, to help everyone out, we share some of our IT Group's monthly information communique, a publication designed to keep employees aware of security risks, issues and relevant things happening in technology.

We begin with the handling of sensitive information. For most banks, sensitive information can be classified into one of four categories: Secret, Confidential, Internal and Public. Each has its role and each is handled differently.

Secret information is the highest level of sensitive company information and as with the military; this information is shared only on a "need to know" basis. Secret information can include passwords, pin numbers, encryption keys and other critical information. Secret data should never be left unattended. When not in use, it should also be encrypted and/or locked in a safe.

Confidential information is sensitive and non-public, but not quite as sensitive as Secret. Examples of Confidential information include account numbers, customer names, addresses, phone numbers, social security numbers, business continuity plans, etc. Confidential information should be protected and should not be left on a desk overnight (clean desk policy). In addition, it should be locked up whenever it is not in use and never be sent outside the company unless it is in encrypted form.

The next level is Internal. This includes data proprietary to the company that is not classified as either Secret or Confidential. As its name suggests, this data is intended for use only within the company and it should be treated as such. Internal information includes org. charts, phone lists, budget, & employee handbook.

The final level is Public. This information includes all data that is in the public domain, carries no restrictions and is available to the general public. Examples of Public information include annual financial reports, business cards & press releases

Now that we all know how to segregate and handle different types of information, we next explore the "clean desk program." Employees should be encouraged and monitored to ensure Secret and Confidential information has been removed every single night from the desk area and locked away. This alleviates the opportunity that someone without authorization can see sensitive information. Locking office doors, desk drawers and doing an office walk around before leaving, are all considered best practices and should be encouraged throughout the bank.

Another key area banks should focus on is related to email usage. Much has been said about the risks of email, but executives should continually remind employees that email communication is not encrypted. We hate to say it, but we still find people sending Secret or Confidential information to others without encrypting it first. Not only is that scary when you think about identity theft, but it is sad because it doesn't have to happen. Anyone sending Secret or Confidential information to anyone

else should encrypt the data before sending it. Setting up a secure data exchange, adding passwords (do not put the password within the same email), monitoring email and ramping up training are all best practices in this area.

As we have outlined, protecting sensitive company and customer information is everyone's job. As one final assist, we close with one very easy thing everyone can do to help things along. Every single time you walk away from the computer, press the "Ctrl, Alt, Delete" keys simultaneously. Then, when the pop-up box appears, press "Lock Computer." This is a simple and effective way to safeguard company information and ensure no one snoops around in your email or files while you are gone. Whether you are a technology guru or not, the simple act of locking your computer when you walk away, is an easy habit to get into and a great way to protect the company.

BANK NEWS

Bank Advertising

Several major banks including BofA and Wells, released full page advertisements in national and local papers essentially telling the public they were strong, are making loans and are committed to helping the economy. If you haven't done so already, you might consider doing something similar in order to aid customer retention, acquisition and brand support.

FASB

The accounting board issued a proposal that would increase the number of times banks issue footnote fair value disclosures from annually to quarterly.

Consumer Stress

The percentage of outstanding credit card balances paid off each month has fallen to 16.1%.

Monitoring

A new study of company monitoring activities finds 80% monitor employee use of company email, 65% review internet activity, 40% observe P2P file sharing, 38% examine instant messaging and 36% check social networking.

Home Sales

The Census Bureau reported Dec. home sales were the lowest in the country since 1963.