

In the wake of global economic turmoil, financial institutions have come under greater scrutiny than ever to provide consumer protection against practices like predatory lending and illegal investment schemes. And they have become a favorite target for data breaches. In fact:

“The financial sector accounted for 93 percent of all such records compromised in 2008.”**

But an ever-present threat exists within every financial organization: database tampering. Despite the most stringent of federal, state and local regulations, the very real possibility that an employee can or will tap into sensitive customer data has not dissipated. And with portable devices such as USB sticks, laptops and handhelds the norm for America’s increasingly mobile workforce, today there are endless ways to transport data out the front door without raising security concerns. Former employees may simply confiscate these devices and never return.

THE NEED FOR DATA ACCESS

Employees within every form of finance—from loan officers and bank tellers to retirement consultants and insurance agents—require access to account numbers, Social Security numbers and credit histories—all information that can easily be used to commit identity theft.

Financial organizations are continually challenged to balance employees’ need for access to sensitive data against the very real possibility that a data breach can occur at any moment.

THE COSTS OF DATA BREACHES

The costs of data breaches, in terms of potential fines, lost profits and lost consumer confidence cannot be overstated. Already today in the US, GLBA (Gramm Leach Bliley Act) regulations require financial institutions to protect themselves against unauthorized access, anticipate security risks, and safeguard a consumer’s nonpublic information. US state rules in Massachusetts (MA 201 CMR 17) and California (CA SB 1386) are mandating the use of encryption to protect data – and Nevada’s NV SB 227 went even further by mandating compliance for the industry-developed Payment Card Industry Data Security

Standard (PCI DSS) for those accepting credit cards. The penalties for non-compliance include stiff civil and criminal penalties, with fines up to \$500,000 per incident for PCI-DSS violations.

TYPES OF DATA LEAKS

Financial organizations that lose sensitive data generally fall into one of three categories:

Those with Legitimate Access Who Store or Share Data Inappropriately: Employees in sales and marketing have legitimate access to company secrets, from product launches to competitive details for a sales pitch. Entire databases can easily be stored on portable media such as USB Thumb Drives in a matter of seconds.

Those With Opportunistic Access: Opportunities to steal data arise everywhere. Someone peeks at a mobile employee’s laptop screen in a train station or airplane. A contractor makes a copy of a hard copy file. A regular employee shares his password with a seasonal employee.

Those Who Have Illegitimate Access: Ex-employees whose access has not been revoked, as well as lost or stolen portable devices, are typically the culprit here.

SET ACCESS CONTROLS

For these reasons, controlling the types of access employees have to sensitive data is critical. Specifically, financial organizations must set controls for:

- › Limiting access to only the data needed to perform the task
- › Which parts of data are accessible
- › What can be done with the data (copy, save, print, etc.)

TAKE PROACTIVE MEASURES

In addition to access controls, the following preventative measures are essential within financial organizations:

Monitor employees’ behavior and set control mechanisms to flag any significant changes.

Employ a detection solution to know when a device is trying to connect to network to sync up with corporate data.

Force-encrypt information when it is removed, legitimately or illegitimately, from the corporate network.

Avoid making unnecessary hard copies of records; never leave them unsecured.

Educate the mobile workforce to the risks posed by their activities and the devices they use.

Revoke all access rights when employees leave.

Never leave a written record of passwords.

Perform background checks on new employees, including contractors and seasonal workers. Conduct regular updates to ensure that nothing has changed.

Never leave data security up to the end user. Whether there is malicious intent or not, employees can easily forget or misunderstand security measures. Centralized control and management helps ensure enforcement and can help lower the total cost of ownership.

Establish corporate governance policies. Compliance is mandated by regulations like GLBA, PCI-DSS and a multitude of state regulations, but responsible data protection doesn't stop there. Every organization should have its own compliance policies in place.

Take control of data protection. Choose a data encryption solution that includes a centralized management console. Your security teams should be able to see that every device is protected.

Get robust reporting capabilities. The best way to achieve safe harbor from disclosing a data breach is having the ability to prove that proper enforcement took place.

A WORD ABOUT ENCRYPTION

It's important to understand that data encryption can take many forms. Here is a brief description of common encryption types.

Encryption – the conversion of data into a form that cannot be easily understood by unauthorized people. Decryption is the process of converting it back to its original form.

Software encryption – encryption accomplished with a software application.

FDE/full-disk encryption – uses disk encryption software to encrypt all the data that goes on a disk or disk volume. It encrypts the entire hard drive, including any blank space.

Hardware encryption – an alternative to software-based, full-disk encryption in which the encryption processing occurs within hardware, and the entire hard drive is encrypted instantaneously.

There are “layers” of encryption as well:

- › User encryption-automatically enforces encryption of user-specific data.
- › File-type encryption-automatically encrypts all new and previously created files of a specified type.
- › Common encryption-automatically encrypts any type of data written to any fixed disk.
- › Application data encryption-encrypts any data written by specified applications, such as MS Word.
- › External media shield encryption-automatic and portable encryption of all media, such as USB sticks, CDs and DVDs.
- › System data encryption-encrypts any data not already encrypted by other policies.

INSIST ON THE FLEXIBILITY TO CHOOSE THE RIGHT SOLUTION

To understand which data encryption solution is right for your organization—and the answer may be a combination of various encryption types—be sure to select a data security provider that will assess your organization's needs and offer the flexibility to choose the best solution, based on your current IT infrastructure, the business size and the business model.

**Verizon Business 2009 Data Breach Study