

NetProtect® Risk Control Bulletin

Protecting Client & Customer Data — It's the Law

RISK CONTROL



Are you the kind of business owner who has every good intention of setting up safeguards for the confidential customer data in your computer system, but just hasn't made time for it? Or are you holding back from investing in or upgrading your system security because other business investments seem more urgent and important for the success of your business?

If so, beware. Protecting client information is NOT optional. It's the law. What's more, a new wave of state privacy laws is setting a higher minimum standard for businesses with custody of confidential client information. In other words, now is the time to ensure that your customer data is protected, because the legal consequences of non-compliance are only going to become more painful.

This bulletin provides an overview of the new laws and the costs to protect confidential client data. Material in the appendix covers the major requirements for safeguarding private personal information. Finally, there is a listing of free computer security tools, along with more detailed information on implementing a comprehensive data security plan.

The New Wave of Privacy Laws

Until recently, the landscape of privacy laws included two types of laws. First, there were breach notification laws at the state level. These laws set forth requirements for notifying clients and mitigating damages in connection with disclosure of personal private information. Second, there were federal "duty to safeguard" laws that generally applied only to certain industries, for instance, the HIPAA Privacy Rule in healthcare and the financial privacy requirements of Gramm-Leach-Bliley.

Now, however, a new wave of laws is raising the stakes on protecting client information. Massachusetts¹, Nevada² and Texas³ recently enacted laws requiring businesses to proactively employ certain minimum safeguards. These laws have a broad reach. If your business has personal

data from anyone living in these states, the laws apply. What's more, the rapid spread of breach notification laws – now on the books in 45 states -- suggests that other states will quickly get on board with the higher standards.

It is also worth noting that while the federal "duty to safeguard" laws apply to specific industries, these new laws apply broadly. Any business that accepts credit card payments or has custody of any other personal private information is subject to their requirements.

In short, any business not making a serious effort to protect personal private information is seriously out of step with the emerging landscape of privacy law. More information in the safeguards required by the new state laws is contained in the appendix of this article.

1. 201 CMR 17.0, Mass general Laws Ch 93 H

2. NRS 597 Sec. 970

3. Business and Commerce Code Sec. 48.102



Personal Private Information

Personal private information generally means an individual's name in conjunction with:

- Social Security Number
- Driver's license number
- State issued ID number
- Financial account number
- Credit or debit card number
- Personal ID or password (i.e., for accessing a network containing financial account information of health information)

Along with client information, businesses are required to protect the personal private information of employees.

Cost of Protection

Chances are that your business has already made some investments in safeguarding client data. Additional costs would depend on how far along you are, and of course, the size and operations of your business.

In general, safeguarding client data doesn't have to be expensive. Advice on establishing data security policies and procedures is widely available, and there are many free tools and services for protecting confidential information. (See additional resources below.)

For small businesses using one or more standalone personal computers, off-the-shelf software is available providing firewalls, antivirus, spam and spyware protection, and encryption. The cost per computer to install and maintain this software is typically only a few hundred dollars. The cost of installing and maintaining this protection in a small computer network is rapidly coming down. Unified Threat Management appliances are firewall routers designed to provide these protections across a small network, typically at a cost of \$1,000 or less.⁴

Summary

The landscape of privacy law is changing rapidly. Until recently, laws were either reactive – dealing with accidental disclosure – or focused on specific industries. The new wave of laws are pro-active – requiring specific safeguards – and broadly applicable to all industries.

When considering the costs and benefits of these safeguards, business owners should consider the consequences of non-compliance. Generally, the states impose statutory fines, penalties or damages for failure to comply. Furthermore, accidental disclosure of private customer information may be even more costly - - notification of clients whose data has been compromised, credit repair services for these clients, litigation and settlements involving clients who have been damaged, not to mention possible regulatory and statutory penalties.

In short, putting off this investment may prove to be “penny wise and pound foolish.”

CNA works with business owners in all industries and we continually communicate on emerging issues and legal trends of data security and privacy laws. To learn more about how CNA Risk Control can work with you to help you protect your customers' confidential data, please speak with your local independent agent, call us toll-free at 866-262-0540 or visit the Risk Control page at www.cna.com/riskcontrol for valuable tools and resources.

January 2009

⁴. http://www.cio.com/article/360514/How_to_Secure_Your_Small_Network



Appendix 1: Critical Safeguards

The new wave of state privacy laws requires safeguards in three broad areas: administrative, physical and technical.

Administrative safeguards are processes and procedures designed to protect private personal information. Critical administrative safeguards include:

Risk Assessment

Identify and assess reasonably foreseeable internal and external risks to confidentiality or integrity of any electronic, paper or other records containing personal information.

Risk Control

Evaluate and improve, where necessary, the effectiveness of your current safeguards for limiting these risks. This includes

- Ongoing employee training – include temp/contract employees
- Monitoring employee compliance with your policies and procedures
- Establishing means for detecting and preventing security system failures.
- Controlling employee access, retention and transportation of records outside of company premises

Risk Avoidance

Limit the amount of personal information that you collect consistent with what is reasonably necessary to accomplish the purpose for which it is collected. This includes limits on the time period over which you retain the information, destruction of non-retained data and restricting access to personal information to employees who need it for business purposes.

Third Parties

- When entrusting personal information to third parties, implement reasonable measures to ensure that they have the capacity to protect this information. This includes:
- Selecting only service providers that are capable of maintaining safeguards for personal information
- Contractually requiring them to maintain such safeguards
- Prior to allowing a service provider to access personal information, insist on written certification that the provider has a written, comprehensive information security program compliant with state law.

Periodic Reviews

Regularly monitor your security program to ensure that it remains effective.

Physical Safeguards are devices and controls that limit physical access to personal private information. Critical safeguards include:

Written Controls

Develop written procedures that establishing the manner in which you restrict physical access to client information.



Secure Storage

Store all such records and data in locked facilities, storage areas or containers.

Technical Safeguards are computer hardware and software tools designed to protect personal private information on your business systems including wireless networks. Critical safeguards include:

User authentication & access controls. These measures relate to user IDs and passwords. They include:

- Secure methods of assigning and controlling access to user IDs and passwords.
- Limiting access to active users and active user accounts
- Blocking access after multiple unsuccessful access attempts, e.g. password or authentication failures

Encryption

This technique converts data into a form that is readable only to those with the proper electronic key. To the extent it is technically feasible, encrypt all transmitted records and files containing personal information that will travel across public networks. In addition, it is critical to encrypt all personal information stored on laptops or other portable devices. Lost or stolen laptops, back-up tapes and other removable media are the leading cause of privacy breaches.⁵ (5. "Chronology of Data Breaches," Available for viewing at <http://www.privacyrights.org/ar/ChronDataBreaches.htm>)

Firewalls & Security Patches

Implement up-to-date firewalls and security patches on any computer or network that is connected to the Internet and that contains personal information.

Virus/spyware Protection

Your software must be up-to-date and configured to automatically receive patches, virus patterns and other security updates on a regular basis.



Appendix 2: Free Tools & Resources

The following are free open-source options for Antivirus protection:

ClamWin - Antivirus program for Microsoft Windows 98/Me/2000/XP/2003 and Vista

<http://www.clamwin.com/>

ClamAV – Antivirus program for UNIX/Linux

<http://www.clamav.net/>

These sources offer free versions of their Antivirus and Anti-spyware tools:

<http://www.comodo.com/> - Comodo offers a variety of free security tools such as personal firewalls, antivirus and anti-spam products.

<http://free.avg.com/> - AVG offers a free antivirus and anti-spyware package.

<http://www.javacoolsoftware.com/spywareblaster.html> - SpyBlaster application prevents installation of spyware.

Vulnerability scanners can be used to search for and map systems for security weaknesses in applications, computers or on a network. Here are two free scanners:

Microsoft Baseline Security Analyzer (MBSA) helps small-and medium-sized businesses who use Microsoft products detect common security misconfigurations and missing security updates on their systems.

<http://technet.microsoft.com/en-us/security/cc184924.aspx>

Tenable Network Security offers free downloads of the **Nessus®** vulnerability scanner, which can be used in detecting security weaknesses through a variety of configuration auditing, sensitive data discovery and vulnerability analysis tools. Subscriptions are required to obtain support, updates to the database of vulnerability checks and compliance auditing.

<http://www.nessus.org/nessus/>

Resources for encryption of stored data:

EFS – The Encrypted File System has been available on professional versions of Microsoft Windows since Windows 2000. EFS allows file level encryption of sensitive files. Additionally, Microsoft BitLocker Drive Encryption is available on Microsoft Windows XP and Vista. With BitLocker, all data on a PC can be encrypted, preventing unauthorized users from being able to circumvent operating system passwords and access data.

The following link is to a “Data Encryption Toolkit for Mobile PCs,” which is provided by Microsoft. This toolkit provides guidance and software tools needed to effectively use both EFS and BitLocker for encryption of sensitive data.

<http://technet.microsoft.com/en-us/library/cc500474.aspx>

TrueCrypt – is a free open-source option for whole disk encryption for Windows Vista/XP, Mac OS X, and Linux operating systems. Details and downloads can be found at the following link:

<http://www.truecrypt.org/>



Email Encryption Resources

Comodo SecureEmail – free application which encrypts and digitally signs email so that they cannot be read by anyone except the intended recipient.

<http://www.comodo.com/>

PGP Desktop Email – offers a free 30 day trial of this e-mail encryption application. The trial also includes whole disk encryption utilities.

http://www.pgp.com/downloads/desktoptrial/desktoptrial2.html#trial_or_freeware

The following are free publications about securing private personal information.

NetProtect Essential Risk Control Primer, available on CNA Risk Control, under Technology, <http://www.cna.com/riskcontrol>

Privacy and Computer Network Security Risks, CNA Risk Control, available on CNA Risk Control, under Technology, <http://www.cna.com/riskcontrol>

Protecting Personal Information: A Guide for Business, Federal Trade Commission, <http://www.ftc.gov/infosecurity/>