

# A/E Network Bulletin

Information and Risk Management Ideas for Design Professionals

## PROTECTING CLIENT & CUSTOMER DATA – IT'S THE LAW

**ARE YOU** the kind of architect or engineer firm 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 firms 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.

### 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. Massachusetts<sup>1</sup>, Nevada<sup>2</sup> and Texas<sup>3</sup> recently enacted laws requiring firms 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 A/E firm not making a serious effort to protect personal private information is seriously out of step with the emerging landscape of privacy law.

### 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, firms are required to protect the personal private information of employees.

### Cost of Protection

Chances are that your firm 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.

For small firms using one or more 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.<sup>4</sup>

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

2. NRS 597 Sec. 970

3. Business and Commerce Code Sec. 48.102

4. [http://www.cio.com/article/360514/How\\_to\\_Secure\\_Your\\_Small\\_Network](http://www.cio.com/article/360514/How_to_Secure_Your_Small_Network)

# PROTECTING CLIENT & CUSTOMER DATA – IT'S THE LAW

(cont. from front)

## 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, firm 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 mean even more costly notification to 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. ♦

For more information on Network Protection for Design Professionals, Schinnerer's new cyber liability endorsement, please contact Cris Vincent at 301-951-6905 or Christine.A.Vincent@Schinnerer.com. You can also visit [www.PlanetNetworkProtection.com](http://www.PlanetNetworkProtection.com) for more program information.



*The information, examples and suggestions presented in this material have been developed from sources believed to be reliable, but they should not be construed as legal or other professional advice. CNA accepts no responsibility for the accuracy or completeness of this material and recommends the consultation with competent legal counsel and/or other professional advisors before applying this material in any particular factual situations. This material is for illustrative purposes and is not intended to constitute a contract. Please remember that only the relevant insurance policy can provide the actual terms, coverages, amounts, conditions and exclusions for an insured. All products and services may not be available in all states and may be subject to change without notice. CNA does not endorse or recommend and makes no representations or warranties as to the accuracy, completeness, effectiveness, suitability, or performance of any of the products, applications, software, or programs identified herein. Any references to non-CNA Web sites are provided solely for convenience and CNA disclaims any responsibility with respect thereto. CNA is a service mark registered with the United States Patent and Trademark Office. Copyright © 2009 CNA. All rights reserved.*