



## CU's Have Plenty of Reasons for Complying With Network Security Regs

*Threats are real and the consequences can be catastrophic.*

By Kelly Dowell  
July 7, 2003

This is the first in a series of articles on online security issues. While it is a major factor, credit unions don't secure their online networks solely to satisfy NCUA regulations. Credit unions secure their networks because the threats from hackers and criminals are real, they pose serious dangers to members' privacy and financial well-being, and the consequences of a cyber-attack can be catastrophic.

The regulations exist because the threats have become serious. They provide some accountability/liability if credit unions don't take standard precautions to secure their networks on their own initiative. That's why a thorough understanding of the regulations can reduce your risk of a successful cyber-attack.

Despite the increasing cyber threat, NCUA regulations wouldn't be as comprehensive as they are today without the legislation that started it all--the Gramm-Leach-Bliley Act.

The Act became effective in November, 2000. The goal of the Act is to make a variety of financial services more readily available to consumers. The Act, also referred to as the Financial Services Modernization Act, consists of various provisions separated into seven chapters or "titles." It's Title V that has sparked the urgency to secure your IT infrastructures.

Making financial services more readily available requires the sharing of consumer information, which in turn obligates your credit union to protect your members' private information. Title V of the Gramm-Leach-Bliley Act introduced consumer privacy requirements that your credit union must now comply. Title V's descriptions and definitions were left broad and general by design. They define your members' private information, who's responsible for protecting it, and the repercussions for *not* protecting it.

Although the Act requires all financial institutions to implement administrative, technical, and physical safeguards to protect customer records and information, it doesn't suggest what to do to protect your networks. This responsibility was

passed on to the individual regulating bodies: the NCUA, FRB, FDIC, OTC, and OCC.

The OCC took the lead in establishing initial rules and guidelines. The NCUA then responded with 12CFR Part 748.

Similar to the Gramm-Leach-Bliley Act, NCUA's Part 748 is general in form. It outlines requirements and provides little in the way of specifics. The appendix to Part 748 provides additional assistance to credit unions by clarifying specific security requirements. Appendix A guidelines require:

- Credit unions must have a written security program plan.
- The board of directors must approve and oversee the institution's security program.
- Credit unions must assess, manage and control their risks.

Your credit union should conduct a risk assessment to manage and control its risk. The risk assessment evaluates your needs, taking into account its size, complexity, technical infrastructure, and the sensitivity of the information maintained.

While the regulations suggest that your credit union's countermeasures should be commensurate with its risk level, examiners are becoming increasingly knowledgeable of security issues. They now realize that minor issues can lead to major risks. Examiners now look for good security practices including policies, physical safeguards, intrusion-monitoring systems, firewalls, anti-virus software, awareness programs, and service-provider oversight.

Although the issue of consumer privacy initiated most of the legislation around online security, the reality is that the risks are more inclusive; i.e., loss of the credit union's computing resources, the compromise of member accounts, and the use of credit union resources to launch outside attacks.

To help credit unions better manage information technology infrastructures and prepare for evolving security risks, NCUA published in December 2002 an [E-Commerce Guide for Credit Unions](#). This guide explains security concerns and processes to help safeguard IT infrastructures. The guide is a good resource for any credit union struggling with online security.

Security will remain an ongoing concern because of the constant, fast-paced evolution in capabilities and complexity of online systems. That's why security isn't a matter of merely fixing an isolated problem and moving on. Rather, it's the challenge of continually limiting your credit union's risks.

For this reason, your credit union shouldn't focus its security efforts exclusively on technical countermeasures like firewalls and anti-virus software. It should focus on managing a complete security program that includes countermeasures.

NCUA documents, such as the appendix to Part 748 and the E-Commerce Guide for Credit Unions, are examples of the agency's regulatory emphasis on process management, not specific fixes.

*(None of the following information should be construed as legal advice. Neither Garrison Technologies nor "The Point for Credit Union Research & Advice" are liable for any use of the information in this article.)*

**About the Author**

**Kelly Dowell**  
CEO  
Garrison Technologies,  
Inc.  
[Kelly@garrison.com](mailto:Kelly@garrison.com)  
512-236-0353 ext.2

This article has been provided to you by *The Point for Credit Union Research and Advice*. If you would like to see more articles related to this topic or other information, visit [thepoint.cuna.org](http://thepoint.cuna.org) for a FREE 30 day trial subscription to *The Point*.