

Simplified GLBA Compliance for Community Banks using Fortinet Hardware, Software and Partner Services

White
Paper



Insights on Complying with Gramm Leach Bliley Act (GLBA)

FORTINET[™]



GLBA compliance is difficult and complex

The Gramm Leach Bliley Act of 1999 puts a tremendous technical burden on all financial institutions, but especially on community banks. Appendix B of the implementing regulations (1) requires that:

*"Each bank shall implement a **comprehensive** written information security program that includes administrative, technical, and physical safeguards **appropriate** to the size and complexity of the bank and the nature and scope of its activities ...A bank's information security program shall be designed to:*

- 1. Ensure the security and confidentiality of customer information;*
- 2. Protect against **any anticipated threats or hazards** to the security or integrity..*
- 3. Protect against unauthorized access to or use...*

(emphasis added)

At no place in the regulations are the terms "comprehensive", "appropriate" or "any anticipated threat" defined or explained. This leaves banks with an open-ended obligation to protect customer data. In an era when cybercrime exceeds illegal drugs as the major source of criminal revenue (2) most small banks are just not technically equipped to deal in-house with the demands of banking and banking security in a computer era (3).

The FFIEC and NIST provide guidance

While the OCC and other regulatory agencies governing community banks have not given clear guidance as to "reasonable" precautions, the Federal Financial Institutions Examination Council (FFIEC) IT Examination Handbook (4) does provide guidance in this area. The FFIEC noted that

*"While no formal industry accepted security standards exist, these various standards provide benchmarks that both financial institutions and their regulators can draw upon for the development of industry expectations and security practices. Some standard-setting groups include the following organizations...**The National Institute of Standards and Technology (NIST) at www.nist.gov**"*

Under the Clinger-Cohen act of 1996 (5) and its successor FISMA, the Federal Information Security Management Act (6) all federal agencies, including the FDIC, OCC etc., must meet information security standards set by the NIST. The agencies are also audited annually on their compliance with NIST standards by the Office of the Inspector General (7).

The following paragraphs show a partial cross listing of NIST standards to the appropriate sections of the GLBA.

12 CFR Part 30 et al, Appendix B to Part 30—Interagency Guidelines Establishing Standards For Safeguarding Customer Information

Information Security Program. Each bank shall implement a comprehensive written information security program ([NIST 800-12](#), [NIST 800-65](#)).

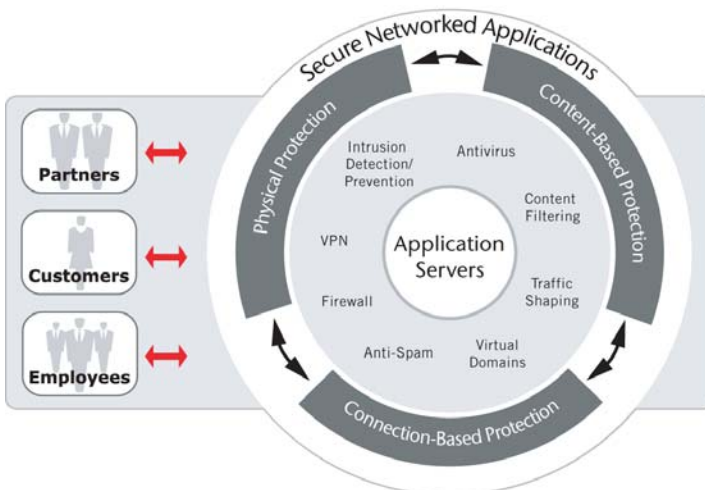
- A. Involve the Board of Directors.*
- B. Assess Risk. ([NIST 800-30](#), [NIST 800-53](#)).*
- C. Manage and Control Risk. ([NIST 800-53](#), [NIST 800-63](#), [NIST 800-73](#), [NIST 800-78](#), [NIST 800-21](#), [NIST 800-61](#), [NIST 800-31](#), [NIST 800-50](#), [NIST 800-42](#)).*
- D. Oversee Service Provider Arrangements. ([NIST 800-42](#), [NIST 800-61](#))*
- E. Adjust the Program.*
- F. Report to the Board ([NIST 800-42](#))*

A more complete cross reference is available on the RLPC website (8)

Fortinet and Fortinet Partners can provide implementation

While the NIST standards are freely available to community banks, their scope (over 1600 pages as of mid-2006) and technical complexity are difficult to manage for a small institution. However, a complete NIST based GLBA compliance program for community banks can be produced at reasonable cost using Fortinet hardware, software and partner services.

There are three types of safeguards listed in the GLBA regulations;



*"Each bank shall implement a **comprehensive** written information security program that includes **administrative**, **technical**, and **physical** safeguards ... all elements of the information security program must be coordinated."*

Administrative safeguards -Fortinet partner RLPC (www.rlpc.net) has produced a software package that reduces the [NIST 800-30](#), [NIST 800-61](#), [NIST 800-53](#) and other protocols to a simple "Turbo-Tax™" style online software package. This program, labeled Secur-Trak™, is continuously updated to reflect the changing security environment, allows banks to incorporate the requirements of the NIST standards without having to master the standards themselves. The software is available as a single package or in a seminar format, with seminars held periodically in both Chicago and Atlanta. The RLPC website seminar page (9) has schedule information for upcoming seminars.

Every year, community banks are required to update their information security programs and risk assessments, including a formal approval by their Board of Directors (10). The seminars held by Fortinet partner RLPC allow banks in a single day to update their programs and meet the ever-expanding regulatory requirements.

A typical community bank risk assessment done according to the NIST 800-30 protocol would include data like the following;

Threat Source	Vulnerability	Impact	Likelihood	Score
Wind	Roof damage	10	0.1	1.0
Fire	Smoke damage, document loss	10	0.5	5.0
Human error	Data retrieval	10	0.1	1.0
Human error	Data modification	50	0.5	25.0
Malicious insider	Data retrieval	100	0.1	10.0
Malicious insider	Data modification	50	0.1	5.0

The numerical scoring is done automatically by the software, and allows easy prioritization of issues.

Current program users are very enthusiastic about the system.

"I am writing to thank you for all of your help with our GLBA compliance. Your software, manual, and assistance were vital in bringing our security standards together and making our regulators happy."

—Timothy L. Wisner MCSE, FCSE, CCNA, MCP+I
Unified Trust Company

"Thank you for your professional updating of our Gramm Leach Bliley Act (GLBA) compliance package. Our new program, based on the continuously evolving standards of the NIST, is far ahead of our old package."

—Michael Hurter, President
BSC Inc.

Physical safeguards - Most banks have adequate vaults, alarms, cameras and locks to deter physical intrusion. Most banks do not have adequate devices, monitoring and software to provide adequate protection against computer intrusion. The Fortinet family of FortiGate™ intrusion prevention systems (IPS) are the award winning newest generation of real-time network protection systems (11). They combine a number of security functions to detect and eliminate the most damaging, content-based threats from e-mail and Web traffic such as viruses, worms, intrusions, inappropriate Web content and more in real time - without degrading network performance. Fortinet products have received over 60 awards since 2001, and Fortinet is the only security company to hold eight ICSA Certifications (12).

Community banks in particular have made excellent use of the FortiGate FG-60 (13). This solid-state unit, named the "Security Product of the Year" in 2004 by Network Computing (14) has continued to be the standard to measure any other product. Robust, fast and highly effective, the FG-60 is an inexpensive and highly effective piece of protective gear. Since late 2000, the OCC has been recommending intrusion detection (15) and it became mandatory for systems meeting federal standards in 2004 (16).

Technical safeguards - Even with the best possible equipment, updating and monitoring network security is a major task that calls on technical skills and resources not commonly found in a small banking environment. BAI Security (17) is a Fortinet partner Managed Security Services Provider (MSSP) that can install, maintain, and monitor bank security on a 24/7 basis. BAI can also provide auditing and reporting services, including the legally required reports on community bank security incidents, annual system status and recommended program improvements.

For banks that already have an effective MSSP, BAI Security can provide auditing and testing services required to meet the "regular testing" provision of the GLBA regulations (18). Whether providing protection to community banks or testing the protection provided by others, BAI Security can provide community banks with the tools they need to protect bank customers.

Summary

The Gramm Leach Bliley Act requires community banks to protect customer information against "any anticipated threats or hazards". This is a major and increasing complex task, as the "hobby hackers" of the '90s give way to the increasing presence of organized crime (19). At a minimum, any bank that outsources its core processing should also consider outsourcing its computer security and GLBA compliance. Half of all community banks outsource processing tasks to allow them to focus on their customers (3). Outsourcing information security tasks allows banks to meet their GLBA obligations and still have time for their customers.



FortiGate Multi-Threat
Security Appliances



FortiManager Central Management and
FortiAnalyzer Logging & Reporting



FortiGuard Security Services and
FortiCare Technical Support

References

1. http://www.ffiec.gov/exam/InfoBase/documents/02-joi-safeguard_customer_info_final_rule-010201.pdf
2. http://www.banklawyersblog.com/3_bank_lawyers/2005/11/cybercrime_bett.html
3. <http://www.kc.frb.org/PUBLICAT/FIP/prs04-4.pdf>
4. http://www.ffiec.gov/ffiecinfbase/html_pages/infosec_book_frame.htm
5. <http://irm.cit.nih.gov/itmra/itmra96.html>
6. <http://csrc.nist.gov/sec-cert/>
7. http://www.oig.doc.gov/oig/archives/about_us/001021.html
8. <http://www.rlpc.net/id12.html>
9. <http://www.rlpc.net/id11.html>
10. http://www.fdic.gov/regulations/examinations/questionnaire/IT_Examination_Officer_Questionnaire.pdf
11. <http://www.fortinet.com/products/>
12. <http://www.fortinet.com/company/advantages.html>
13. <http://www.fortinet.com/doc/FGT60DS.pdf>
14. <http://fortinet.com/news/pr/2004/pr051104.html>
15. http://www.occ.treas.gov/efiles/disk2/resources/info_sec/occ-bul_2000_14_infrastructure_threats_intrusion_risks.pdf
16. <http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf>
17. http://www.baisecurity.com/news_2.asp?ArticleID=19
18. <http://www.baisecurity.net/auditing.asp> 19. http://www.foxnews.com/printer_friendly_story/0,3566,191375,00.html

About RLPC

Since 1993 RLPC has been at the interface between compliance and technology, helping businesses worldwide use the latest technology to meet regulatory needs. RLPC provides information security and regulatory compliance services to the medical, commercial and financial industries worldwide. Services also include preparation of information security and contingency plans, network upgrades and audit preparation.

About Fortinet

Fortinet is the pioneer and leading provider of ASIC-accelerated multi-threat security systems, which are used by enterprises and service providers to increase their security while reducing total operating costs. Fortinet solutions were built from the ground up to integrate multiple levels of security protection--including firewall, antivirus, intrusion prevention, Web content filtering, VPN, spyware prevention and antispam--providing customers a way to protect multiple threats as well as blended threats. Leveraging a custom ASIC and unified interface, Fortinet solutions offer advanced security functionality that scales from remote office to chassis-based solutions with integrated management and reporting. Fortinet solutions have won multiple awards around the world and are the only security products that are certified eight times over by the ICSA (firewall, antivirus, IPSec, SSL, IDS, client antivirus detection, cleaning and antispayware). Fortinet is privately held and based in Sunnyvale, California.

FORTINET

1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1-408-235-7700 Fax +1-408-235-7737
www.fortinet.com

©2006 RLPC. All rights reserved. Used with permission of RLPC. The names of actual companies and products mentioned herein may be the trademarks of their respective owners. Licensed under U.S. Patent No. 5,623,600

WPR127-0806-R1