Endpoint Security Considerations for Achieving GLBA Compliance
Contents

Fixing the Financial System Includes
Strong Safeguards for Customer Information ........................................... 3
Overview of GLBA Security Requirements ................................................. 3
Planning for GLBA Endpoint Compliance ................................................ 3
Technologies for Endpoint Security .......................................................... 4
Best Practices for Deploying Endpoint Security ........................................ 4
Endpoint Security Controls for GLBA Compliance ................................... 4
Learn More ............................................................................................... 5
Fixing the Financial System Includes Strong Safeguards for Customer Information

Rebooting the global financial system may take years. The international move to new regulatory organizations will require financial institutions to change the way they do business. No one knows exactly how the system will change yet, but one thing is certain: financial institutions will be required to protect the security and confidentiality of customer information. The Gramm-Leach-Bliley Act (GLBA) of 1999 (P.L. 106-102) defines guidelines and standards for safeguarding customer information. These rules apply to all financial institutions doing business in the U.S. New laws and financial regulations for the coming reboot may change GLBA, but increasing threats to customer data will only guarantee tighter security requirements. In gauging threats to the security of customer information, unprotected endpoints constitute the largest source of potential breaches in financial institutions. GLBA provides guidance for addressing security threats to endpoints.

Overview of GLBA Security Requirements

Congress enacted GLBA as a broad effort to improve financial services targeting consumers. The banking industry was first to publish security guidelines for financial institutions and the GLBA Safeguards Rule and audit guidelines are based directly on these efforts. GLBA security provisions are mandatory for all institutions offering financial products and services to individuals. Both federal and state governments enforce these rules and organizations that do not comply will face potential administrative actions, fines, or criminal prosecution.

The GLBA Safeguards Rule specifies three kinds of safeguards or controls required by financial institutions when implementing security:

- **Administrative Safeguards**—financial institutions must document formal policies and practices for data protection, including the organization’s security management process, and implementation specifications.

- **Physical Safeguards**—financial institutions must protect customer data from the hazards of fire, weather, environment and intrusion.

- **Technical Safeguards**—financial institutions must control direct access to information by individuals, and must also guard against unauthorized access via a network.

Planning for GLBA Endpoint Compliance

Endpoints are the universal ‘Achilles heel’ of risk for GLBA security compliance. Attacks increasingly bypass traditional perimeter-focused security and enter endpoints and the financial organization network by many vectors. Mobile endpoints may be used outside the traditional perimeter of security controls. And it’s difficult to manually ensure that all controls required for compliance are always operating effectively on every endpoint. Automation is vital. Choosing and using the right endpoint security technical controls is a key part of the GLBA compliance process.
Technologies for Endpoint Security

Deployment of standard endpoint security technologies will provide a robust and comprehensive multi-layer defense against exploits. These are essential security controls for verifying compliance with GLBA and other regulations.

<table>
<thead>
<tr>
<th>Essential endpoint security technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Firewall</strong> — Blocks or allows traffic based on criteria defined by endpoint security policies.</td>
</tr>
<tr>
<td><strong>Intrusion Detection / Prevention System</strong> — IDS/IPS technology analyzes network traffic for malicious code and attacks.</td>
</tr>
<tr>
<td><strong>Program Control</strong> — Restricts network access on a per-program basis thereby limiting exposure to vulnerabilities and attacks.</td>
</tr>
<tr>
<td><strong>Network Access Control</strong> — NAC restricts access by unknown users by enforcing policy compliance at endpoints and offering auto-remediation.</td>
</tr>
<tr>
<td><strong>Antivirus / Anti-spyware</strong> — Automatically scans files based on a variety of criteria to identify viruses and malware, and responds according to policy.</td>
</tr>
<tr>
<td><strong>Data Security</strong> — Protects data stored on endpoints through a combination of user authentication, data encryption and port control.</td>
</tr>
<tr>
<td><strong>Secure Remote Access</strong> — Establishes a virtual private network (VPN) allowing remote users to safely access corporate resources.</td>
</tr>
</tbody>
</table>

Best Practices for Deploying Endpoint Security

**Deploy integrated solutions** — Choose solutions from reputable vendors that address multiple requirements. Integrated solutions can optimize management and administration efficiencies. This may not be possible with individual point solutions.

**Be holistic** — Deploy solutions that address core security capabilities and facilitate compliance with multiple regulations and industry guidelines.

**Add value** — Use solutions that enhance fundamental business value and differentiate your business, such as adding new sales channels.

**Ensure future scalability** — Deploy solutions that will adapt to and grow with changing business requirements.

<table>
<thead>
<tr>
<th>Endpoint Security Controls for GLBA Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GLBA Requirement</strong></td>
</tr>
</tbody>
</table>
| Access controls on customer information systems. [Appendix B, III(C)(1)(a)]  
  • To authenticate and permit authorized access to customer information. | Endpoint access control automatically regulates network access. Endpoint program control technology provides granular application access control. |
| Encryption of electronic customer information in storage or transit. [Appendix B, III(C)(1)(c)]  
  • Selection of data to encrypt. The encryption technique and level should be supported by the risk assessment. | Endpoint encryption solutions provide automatic full disk encryption, media encryption, and encryption for mobile devices such as laptops, personal digital assistants and smart phones. |
| Procedures to ensure that customer information system modifications are consistent with the bank’s information security program. [Appendix B, III(C)(1)(d)]  
  • Specify who can make hardware and software changes to the system. | Endpoint access control technology automatically regulates network access. Endpoint program control technology provides granular application access control. Endpoint firewall restricts or allows network activity. |
Monitoring systems and procedures to detect actual and attempted attacks on, or intrusions into customer information systems.  
[Appendix B, III(C)(1)(f)]  
- Network and host intrusion detection systems.  
- Network traffic monitoring.  
- Manual review of logs and other information available to assess management’s monitoring processes.

<table>
<thead>
<tr>
<th>Best practices such as COBIT specify use of all standard endpoint protection controls including firewall, intrusion-detection / prevention systems (IDS/IPS), program control, network access control, antivirus &amp; anti-spyware, data security, and remote access control.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDS/IPS technologies must include each endpoint that can access customer information. Endpoint IDS/IPS must be integrated with the organization’s standard security alert system. Endpoints must automatically post security events to audit log files.</td>
</tr>
</tbody>
</table>

Response programs that specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to the customer information systems.  
[Appendix B, III(C)(1)(g)]

<table>
<thead>
<tr>
<th>Endpoint policy compliance is enforced by network access control technology, such as checking endpoints for the latest version of anti-virus software, and auto-remediating endpoints into compliance before allowing access to systems with protected data.</th>
</tr>
</thead>
</table>
| Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards or technological failures.  
Appendix B, III(C)(1)(h)]

<table>
<thead>
<tr>
<th>Endpoint data protection technology should automatically create a centrally-stored recovery file for disaster recovery.</th>
</tr>
</thead>
</table>
| Regularly test the key controls, systems and procedures of the information security program.  
[Appendix B, III(C)(0)]

| Reports from endpoint policy compliance technology must document that each endpoint is operating all mandated security controls and the most current security software. |

Learn More
For more information about the Gramm-Leach Bliley Act visit the FTC Web site:  
http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

For more information about Standards for Safeguarding Customer Information visit:  

To learn how Check Point Endpoint Security solutions can help you achieve GLBA compliance, please contact your local Check Point sales representative, call Check Point at 800-429-4391, or visit:  
www.checkpoint.com/products/datasecurity/index.html
About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leader in securing the Internet. The company is a market leader in the worldwide enterprise firewall, personal firewall, data security and VPN markets. Check Point’s PURE focus is on IT security with its extensive portfolio of network security, data security and security management solutions. Through its NGX platform, Check Point delivers a unified security architecture for a broad range of security solutions to protect business communications and resources for corporate networks and applications, remote employees, branch offices and partner extranets. The company also offers market leading data security solutions through the Pointsec product line, protecting and encrypting sensitive corporate information stored on PCs and other mobile computing devices. Check Point’s award-winning ZoneAlarm Internet Security Suite and additional consumer security solutions protect millions of consumer PCs from hackers, spyware and data theft. Extending the power of the Check Point solution is its Open Platform for Security (OPSEC), the industry’s framework and alliance for integration and interoperability with “best-of-breed” solutions from hundreds of leading companies. Check Point solutions are sold, integrated and serviced by a network of Check Point partners around the world and its customers include 100 percent of Fortune 100 companies and tens of thousands of businesses and organizations of all sizes.

CHECK POINT OFFICES

Worldwide Headquarters
5 Ha’Solelim Street
Tel Aviv 67897, Israel
Tel: 972-3-753 4555
Fax: 972-3-624-1100
email: info@checkpoint.com

U.S. Headquarters
800 Bridge Parkway
Redwood City, CA 94065
Tel: 800-429-4391; 650-628-2000
Fax: 650-654-4233
URL: http://www.checkpoint.com

©2009 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Endpoint Security On Demand, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Full Disk Encryption, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQEngine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSG, Firewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Power-1, Provider-1, PureAdvantage, PURE Security, the puresecurity logo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecuTurbocard, Security Management Portal, Sentinel, SiteView, pop-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smart Meter, Smart-M, SmartMap, SmartPortal, SmartProvisioning, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartView Tracker, SMR, SMP On-Demand, SotaWaris, SSL Network Extender, Stateful Clustering, Total Security, the totalsecurity logo, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, UTM-1 Total Security, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VX, VX-1, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm ForceField, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates, ZoneAlarm is a Check Point Software Technologies, Inc. Company. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 5,987,611, 6,496,935, 6,873,988, 6,850,943, and 7,165,076 and may be protected by other U.S. Patents, foreign patents, or pending applications.

March 19, 2009