CORE Security and GLBA

Addressing the Graham-Leach-Bliley Act with Predictive Security Intelligence Solutions from CORE Security
Introduction

The Gramm-Leach-Bliley Act (GLBA) of 1999 was enacted in response to the rapid increase in Internet banking and online access to account information. GLBA Section 501(b), titled “Establishing Standards for Safeguarding Customer Information,” requires financial institutions in the United States to create information security programs that:

- Ensure the security and confidentiality of customer information;
- Protect against any anticipated threats or hazards to the security or integrity of such information; and,
- Protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.

Penalties for non-compliance include fines to businesses of up to $100,000 per violation, fines for officers and directors of up to $10,000 per violation, criminal penalties of up to five years in prison, and revocation of professional licenses.

GLBA doesn’t prescribe any technologies or exact guidelines of developing such a program to safeguard customer information and integrity. Instead, the Federal Financial Institutions Examination Council (FFIEC), comprised of examiners from many different regulatory bodies, is tasked with GLBA enforcement. The FFIEC IT Examination Handbook and the FFIEC “Authentication in an Internet Banking Environment” supplement – as well as numerous enterprise risk management frameworks prescribed by COSO, COBIT and NIST – assists auditors with exhaustive tests to assess compliance with GLBA Section 501b.

The examination steps for Section 501(b) include the following considerations:

- Involvement of the board in overseeing and designing the corporate information security program
- Evaluation of the risk assessment process
- Evaluation of the adequacy of the program to manage and control risk
- Assessment of measures to oversee service providers
- Process to adjust the information security program
- Communication of findings

Addressing GLBA Requirements with CORE Security Solutions

IT security guidance from the FFIEC provides risk professionals and auditors the necessary best practices to fulfill and enforce GLBA Section 501b. Predictive security intelligence solutions from CORE Security address much of the FFIEC guidance as detailed in the table on the following pages.
### FFIEC Guidance and How CORE can help

#### Information Security Risk Assessment (from FFIEC IT Examination Handbook)

Financial institutions must maintain an ongoing information security risk assessment program that effectively:

- Gathers data regarding the information and technology assets of the organization, threats to those assets, vulnerabilities, existing security controls and processes, and the current security standards and requirements;
- Analyzes the probability and impact associated with the known threats and vulnerabilities to their assets; and
- Prioritizes the risks present due to threats and vulnerabilities to determine the appropriate level of training, controls, and assurance necessary for effective mitigation.

#### Conduct Proactive, Real-World Risk Assessments

Our predictive security intelligence solutions enable financial institutions to proactively identify critical threats, see how risk changes over time as technology and business processes evolve, and prioritize their risk and security practices to stay ahead.

- Continuously assess changing infrastructure against the latest threats and proactively identify weaknesses posing imminent risks
- Leverage automation and delegation to increase the scale and frequency of security assessments across large IT environments
- Add deeper intelligence and context to vulnerability and threat data through actual testing and simulation; enabling security and risk teams to prioritize and remediate the most critical threats.

#### Risk Assessments (from “Authentication in an Internet Banking Environment” supplement)

Institutions must establish a Risk Assessment that accounts for:

- Constantly evolving threats to both its internal and external environment
- Changes to how customers utilize online banking systems, or when new services are introduced
- Actual security incidents which occur within the institution and industry

The Risk Assessment must be reviewed, updated or performed at least every 12 months

#### Information Security Strategy (from FFIEC IT Examination Handbook)

Financial Institutions should develop a strategy that defines control objectives and establishes an implementation plan, including appropriate considerations of prevention, detection, and response mechanisms as well as layered controls that identify threats to organizational assets.

#### Build Risk Preemption into Your Security Strategy

- Prevent and proactively defend against newer types of threats such as malware and advanced persistent threats through real world replication and simulation of attacks
- Conduct multi- and cross-vector analysis across web applications, network systems, and endpoints to identify exposures across layered controls and
<table>
<thead>
<tr>
<th><strong>FFIEC Guidance</strong></th>
<th><strong>How CORE can help</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security Controls Implementation (from FFIEC IT Examination Handbook)</strong></td>
<td>access to organizational assets such as IP or customer data</td>
</tr>
<tr>
<td>An effective control mechanism includes numerous controls to safeguard and limits access to key information system assets at all layers in the network stack. This section addresses logical and administrative controls, including access rights administration for individuals and network access issues.</td>
<td>• Reduce the overall response and remediation time by alerting security and downstream IT teams to the highest priority vulnerabilities</td>
</tr>
<tr>
<td><strong>Layered Security Controls (from “Authentication in an Internet Banking Environment” supplement)</strong></td>
<td>Verify Security Controls Efficacy</td>
</tr>
<tr>
<td>Institutions should implement a strategy of Layered Security to protect online transactions:</td>
<td>FFIEC guidance acknowledges that diverse security controls at different points in a transaction flow can help mitigate weaknesses. Most banks also realize that single layer of authentication will simply not work with constant change and myriad of technologies.</td>
</tr>
<tr>
<td>• Use different controls at different points in a transaction to help mitigate any weaknesses</td>
<td>As a result, CISOs and CROs must grapple with multiple layers of security technologies – and somehow consolidate and understand the data they provide. CORE solutions offer continuous and consistent application to monitoring and assessment to keep up with diverse controls environments.</td>
</tr>
<tr>
<td>• Use a risk-based approach where controls are strengthened as risk increases</td>
<td>• Continuously assess large, diverse IT environments</td>
</tr>
<tr>
<td>• Deploy processes that detect and respond to suspicious activities at the riskiest points of online transactions</td>
<td>• Assess IPS/IDS, firewalls and other defenses against real-world network, client-side and web application attack techniques</td>
</tr>
<tr>
<td>• Enhance the controls over system administrators who manage online access and configurations of commercial accounts</td>
<td>• Ensure that defensive technologies are configured and updated to protect against current threats</td>
</tr>
<tr>
<td>Use the results of the Risk Assessment to adjust levels of authentication controls accordingly.</td>
<td>• Reveal paths that attackers and malicious insiders would use to circumvent security controls and access sensitive assets</td>
</tr>
<tr>
<td></td>
<td>• Maintain asset visibility by automatically sensing and adapt to changes in infrastructure</td>
</tr>
<tr>
<td></td>
<td>• Repeat assessments to validate the efficacy of new or updated security controls</td>
</tr>
<tr>
<td><strong>Security Threat &amp; Process Monitoring &amp; Updating (from FFIEC IT Examination Handbook)</strong></td>
<td>Stay Ahead of Evolving Threats</td>
</tr>
<tr>
<td>Financial institutions should continuously gather and analyze information regarding new threats and vulnerabilities, actual attacks on the institution or others, and the effectiveness of the existing security controls. They should then use that information to update the risk assessment, strategy, and</td>
<td>Things change -- Financial institutions should validate their ongoing risk mitigation strategy and processes by monitoring network and host activity to identify policy violations, anomalous behavior, unauthorized configuration, and other conditions that increase risk. They should also analyze the results of monitoring to accurately and quickly identify, classify, escalate, report</td>
</tr>
</tbody>
</table>

4
<table>
<thead>
<tr>
<th>FFIEC Guidance</th>
<th>How CORE can help</th>
</tr>
</thead>
<tbody>
<tr>
<td>implemented controls.</td>
<td>and guide responses to security incidents.</td>
</tr>
</tbody>
</table>

CORE solutions enable financial institutions to:

- Assess systems designated as critical and delivers proactive alerts regarding the latest threats and impacts to those systems
- Assimilate data from multiple sources (e.g., network and web scanners) to validate potential threats as real
- Pinpoint what is truly exploitable, enabling smarter decisions to prioritize and escalate remediation actions.
- Deliver data using terminology specific to the organization, system, location, mandates, data types, etc.
- Validate security metrics; benchmark & track risk posture

About CORE Security

CORE Security is the leading provider of predictive security intelligence solutions. We help more than 1,400 customers worldwide preempt critical security threats and more effectively communicate business risk. Our award-winning enterprise solutions are backed by over 15 years of expertise from the company’s CORE Labs research center. Learn more at www.coresecurity.com.