# PatchLink Security Configuration Management™

The Gramm Leach Bliley Act of 1999 (GLBA) sets a very high standard for information security. Under CFR § 314.3

> "You shall develop, implement, and maintain a comprehensive information security program that …contains administrative, technical, and physical safeguards that are appropriate…

"Comprehensive" and "appropriate" are strong words in the current security climate. Today, cybercrime exceeds illegal drugs as the world's number one crime and "reasonably foreseeable internal and external risks" covers a wide range of hazards. Information systems are under attack on a daily basis, and even small mistakes can be costly; one misconfigured firewall can allow access to an entire network of customer information. For example, 45 million customer records from retailer TJX were compromised due to a single poorly secured wireless router.

A significant problem in GLBA compliance is determining what constitutes a "reasonably forseeable" risk. National Institute of Standards and Technology (NIST) guidance provides a cost effective answer. NIST Special Publication 800-30, the Risk Management Guide for Information Technology Systems, lays out a risk management system with three major elements;

1. **Characterize** the information systems
2. Analyze, select and implement **safeguards**
3. **Assess and report risks**

## Patchlink Security Configuration Management™ (SCM) makes GLBA compliant risk assessments easy.

PatchLink technology provides support for all three of the basic GLBA compliance tasks. PatchLink Scan™ provides continuously updated system **characterization**. Patchlink SCM™ provides a comparison of existing **safeguards** with NIST 800-53 requirements and uses the configuration and safeguard information to automatically **calculate and report risks** to protected information.

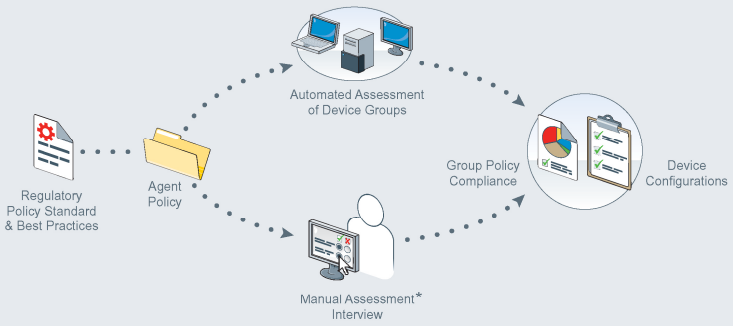
### How It Works and What It Can Monitor

**Policy Import**
Import of policy standards according to SCAP checklists (e.g. FDCC).

**Automated Assessment**
Used with PatchLink Update™ or PatchLink Scan™, automated assessment against the checklist is performed.

**Manual Assessment***
In order to be exhaustive, manual assessment Interview allows the mapping of non-IT automated security checks such as physical security checks.

**Policy Compliance Management & Reporting**
Both automated assessment and manual assessment interview checks are consolidated to provide a comprehensive compliance monitoring and reporting tools




- Event Log Policy Settings
- File Permission Settings
- Local policies Group
- System Services Group
- Network Settings
- System Settings
- Windows Components
- Local User Policy Settings
- Security Patches
- Firewall Settings
- IE Settings
- Application Settings

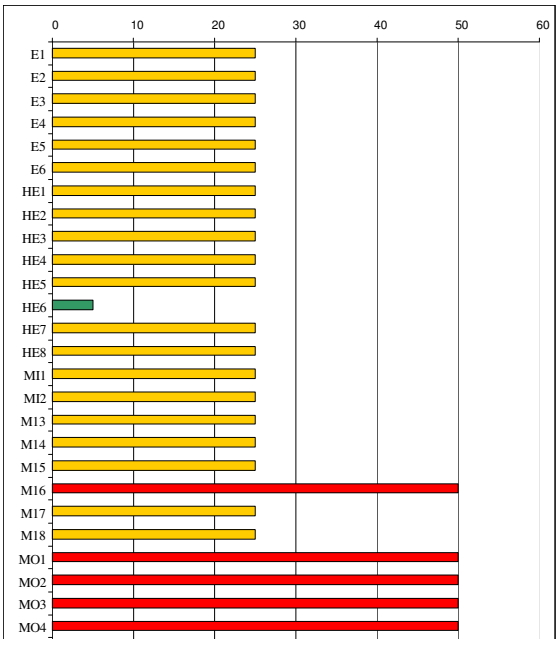
The easily interpreted reports can rapidly communicate changes in risks to protected information. The automated risk assessment reports can be updated as often as daily, with alarms sent by text message or email when risks increase beyond pre-set limits.

PatchLink SCM™ utilizes SCAP validated scanning and Policy Questionnaire data (shown below) to generate NIST compliant risk assessments.

| Question | Description | Answer |
|---|---|---|
| IR-1 | **IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES**<br>The group writes an incident response policy. It must be given to all employees and be reviewed and updated at least once a year.<br>The policy states why it is needed, to whom it pertains, and who will take an active role in incident response.<br>The group writes procedures that will state how it will handle incident response and what controls will be in place.<br>The incident response policy and procedures comply with all laws and rules for the group's industry.<br>The incident response policy can be included as part of the general information security policy for the group. Incident response procedures can be written for the security program in general, and for a specific computer system. | Yes |

The output of the combined automated/manual PatchLink assessment process provides a continuously updated picture of network compliance with standards provided by the NIST. Risk assessment data can be expressed numerically or graphically, as shown below.

| | Threat Source | Vulnerability | Likelihood | Impact | Baseline Score |
|---|---|---|---|---|---|
| E1 | Wind | Roof damage | M | M | 25 |
| E2 | Fire | Smoke damage | M | M | 25 |
| E3 | Flood | Facility damage | M | M | 25 |
| E4 | Power loss | Loss of operations | M | M | 25 |
| E5 | Power loss | Damage to building | M | M | 25 |
| E6 | Vehicle collision | Facility damage | M | M | 25 |
| HE1 | Human error | Data acquisition | M | M | 25 |
| HE2 | Human error | Data storage | M | M | 25 |
| HE3 | Human error | Data retrieval | M | M | 25 |
| HE4 | Human error | Data modification | M | M | 25 |
| HE5 | Human error | Data transmission | M | L | 25 |
| HE6 | Human error | System design | M | M | 5 |
| HE7 | Human error | Procedure implementation | M | M | 25 |
| HE8 | Human error | Internal controls | M | M | 25 |
| MI1 | Malicious insider | Data acquisition | M | M | 25 |
| MI2 | Malicious insider | Data storage | M | M | 25 |
| M13 | Malicious insider | Data retrieval | M | M | 25 |
| M14 | Malicious insider | Data modification | M | M | 25 |
| M15 | Malicious insider | Data transmission | M | H | 25 |
| M16 | Malicious insider | System design | M | M | 50 |
| M17 | Malicious insider | Procedure implementation | M | M | 25 |
| M18 | Malicious insider | Internal controls | M | H | 25 |
| MO1 | Malicious outsider | Data acquisition | M | H | 50 |
| MO2 | Malicious outsider | Data storage | M | H | 50 |
| MO3 | Malicious outsider | Data retrieval | M | H | 50 |
| MO4 | Malicious outsider | Data modification | M | H | 50 |
| MO5 | Malicious outsider | Data transmission | M | H | 50 |
| MO6 | Malicious outsider | System design | M | L | 50 |
| MO7 | Malicious outsider | Procedure implementation | M | L | 5 |
| MO8 | Malicious outsider | Internal controls | L | L | 1 |




A significant challenge for information system managers is dealing with service providers that need access to protected information. Under the GLBA, information owners are required to ensure that service providers supplied with protected data must be “capable of maintaining appropriate safeguards for the customer information at issue”. Reporting using the PatchLink SCM technology can provide continuously updated risk assessments for each service provider.

| ID | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| Date | 10/10/07 | 10/11/07 | 10/11/07 | 10/12/07 | 10/12/07 | 10/12/07 |
| Risk | GO! | GO! | GO! | GO! | GO! | GO! |
| E1 | 25 | 50 | 25 | 25 | 25 | 100 |
| E2 | 50 | 50 | 50 | 50 | 50 | 100 |
| E3 | 50 | 50 | 25 | 50 | 25 | 100 |
| E4 | 1 | 50 | 50 | 5 | 50 | 100 |
| E5 | 5 | 50 | 50 | 5 | 50 | 100 |
| E6 | 5 | 25 | 25 | 5 | 25 | 50 |
| HE1 | 25 | 25 | 25 | 25 | 25 | 25 |
| HE2 | 25 | 25 | 50 | 25 | 25 | 25 |

GLBA compliance with the information safeguards rule is a constant challenge.. Patchlink Security Configuration Management™ tools can make meeting the challenge more possible and less expensive. lower cost is imperative.

For more information on Security Configuration Management™ or other PatchLink products, contact your Lumension representative or go to www.lumension.com.