

## PAETEC'S POSITION ON SECURITY COMPLIANCE

### Compliance In General

Our customers are under increasing pressure to adhere to numerous security compliance standards and design networks that address the best practices associated with these standards. As any healthcare provider can tell you, the content of the standards themselves can be daunting to understand and apply, which has driven organizations to look outside for assistance.

#### Top Five Industry Compliance Standards

- Payment Card Industry Digital Security Standard (PCI DSS) – Applies to any company processing, transporting, or storing credit card information

- Government Mandated Privacy Acts (Massachusetts, California, and Minnesota, with others to follow) – Applies to anyone doing business in these states
- Health Insurance Portability and Accountability Act (HIPAA) – Applies to the healthcare vertical
- Gramm-Leach-Bliley Act (GLBA) – Applies to the financial vertical
- Sarbanes-Oxley Act (SOX) – Applies to public companies

### Overview of Standards

**PCI DSS** – The goal of PCI DSS is to create a framework for good security practice around the handling of cardholder data. A PCI-compliant operating environment is one in which the cardholder data exists (i.e., it does NOT refer to the whole corporate network), and PCI DSS defines the requirements for how access to this data must be controlled, monitored, logged, and audited.

**Government Mandated Privacy Acts (Massachusetts)** – The Massachusetts Data Privacy Act (201 CMR 17), now recently revised, went into effect March

1, 2010. It applies generally to those businesses that own or license personal information about Massachusetts residents. Personal information includes Massachusetts residents' first and last names, or first initials and last names, in combination with any of the following: Social Security number, driver's license number or state-issued identification card number, financial account number, or credit or debit card number. Therefore, if you have any employees, receive payments from individuals (whether by check or credit card), or send out 1099s, your business owns or licenses personal

## Overview of Standards (Cont.)

information and, thus, must comply with the law. Minnesota and California recently passed similar laws and it's expected that this trend will continue for the remaining 47 states in the near future.

**HIPAA** – HIPAA covers a number of healthcare standards, one of which is the HIPAA Security Rule, which requires implementation of three types of safeguards:

- Administrative
- Physical
- Technical

In addition, it imposes other organizational requirements and a need to document processes analogous to the Privacy Rule. Implementing within and adhering to this rule is extremely difficult due to the highly technical nature of the contents of the rule.

**GLBA** – The Safeguards Rule, a part of the GLB Act, requires financial institutions to develop a written information security plan that describes how the company is prepared for, and plans to continue to protect clients' non-public personal information. (The Safeguards Rule applies to information of any consumers past or present of the

financial institution's products or services.)

**This plan must include:**

- Denoting at least one employee to manage the safeguards
- Constructing thorough risk management on each department handling the non-public information
- Developing, monitoring, and testing a program to secure the information
- Modifying the safeguards as needed with the changes in how information is collected, stored, and used

This rule is intended to do what most businesses should already be doing: protecting their clients. The Safeguards Rule forces financial institutions to take a closer look at how they manage private data and to do a risk analysis on their current processes. No process is perfect, so this has meant that every financial institution has had to make some effort to comply with the GLBA.

**SOX** – The impact of IT security within SOX is somewhat indirect since the law is primarily focused on the accuracy of financial reporting data. IT security is important under SOX only to the extent that it enhances the reliability and integrity of that reporting.

## PAETEC's Strategy Around Compliance

The Internet Service Provider (ISP) has an interesting role in compliance. Since the essential underlying focus of popular compliance standards today is on individual enterprise context, it's impossible for PAETEC to provide "instant on" compliance. However, with our Security Consultation services, as well as the best practices that we've implemented internally and consult our customers to follow, PAETEC has made it as easy as possible for customers from all verticals to meet and exceed the standards laid out for them by the various regulatory bodies. Each compliance standard is built around a foundation of concepts best outlined by the SANS Institute and mirrored by PAETEC's business best practices. They include:

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
4. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
5. Boundary Defense
6. Maintenance, Monitoring, and Analysis of Audit Logs
7. Application Software Security
8. Controlled Use of Administrative Privileges
9. Controlled Access Based on Need to Know
10. Continuous Vulnerability Assessment and Remediation
11. Account Monitoring and Control

12. Malware Defenses
13. Limitation and Control of Network Ports, Protocols, and Services
14. Wireless Device Control
15. Data Loss Prevention
16. Secure Network Engineering
17. Penetration Tests and Red Team Exercises
18. Incident Response Capability
19. Data Recovery Capability
20. Security Skills Assessment and Appropriate Training to Fill Gaps

Furthermore, PAETEC is actively taking advantage of the SAS 70 auditing process to provide customers with the necessary information to inform their auditors and planners of compliance-friendly topologies and practices. A SAS 70 is performed by a third party that reviews our security controls, then verifies that we're adhering to them by reviewing, auditing, and scoring our performance. Since our customers are under a myriad of compliance standards, we developed our controls based upon the best practices mentioned above and mapped our practices to PCI DSS and other compliance standards. This way, we can present our SAS 70 documentation to any customer who needs to prove that PAETEC practices security standards which exceed the compliance standards to which they're being held. This approach makes the most sense for both PAETEC and our customers.

## Things We're Watching & What We're Doing

Since PAETEC's role is central to customer network security, we as an ISP and Managed Security Service Provider (MSSP) must be "ahead of the curve" to maintain our position within the confines of the popular compliance standards because the overwhelming buying triggers for our services surround these standards. We see emerging threats and general business practices that require review and standards application on a regular basis.

### Top Three Emerging Trends

- Best practices surrounding safe and secure utilization of social media
- Best practices incorporating enclaving of network elements to reduce the impact of a breach or incident
- Best practices surrounding the deployment, control, and risk mitigation associated with mobile technology (Android, iPad, iPhone, WiFi, etc.)

**Social Media** – Malware and bot-net threats are synonymous with social media. While it's a well known best practice to develop Web acceptable use policies that block access to these services, an increasing number of organizations use social media as an advertising and information distribution outlet. With this

trend, there are a number of best practices and technologies that we're focusing on to control access, then monitor and equip zones within the organization with legitimate access to these services to properly handle threats.

**Enclaving** – There is no 'silver bullet' in security. If there were, this multi-billion dollar industry would not exist. Given that reality, it's becoming increasingly more prudent to design networks (LAN and WAN) that are zoned (or enclaved) in such a way that in the event of a successful attack or breach, the impact to the organization as a whole is minimized. As threats grow in complexity, best practices around this concept are increasing in value.

**Mobile Devices** – Innovation and incorporation of mobile devices is skyrocketing across all industries. Mobile device security, as a result, is becoming a targeted focus for our customers and our organization. The development of best practices and the deployment of security technology with a focus on mobile device risk reduction and mitigation is a top priority at PAETEC.