Networking Compliance

A White Paper

November 2011

Contents

Compliance today

Introduction

Information technology (IT) has grown to fundamentally change the way we do business, in terms of scale, speed and scope. Advances in IT have resulted in new services and new capabilities that would have been unimaginable only 20 years ago, and affect virtually everything from the way we handle our healthcare or finances to the way corporations are organized. Consumers now have remarkable access to information, while organizations strive to make their operations increasingly transparent.

At the same time, innovations in IT have also resulted in new demands placed on the network and have added new threat vectors to corporate and consumer information. The result is a myriad of international, federal, state, local and industry regulations, designed to help ensure security and privacy of data and resources. Most organizations are subject to more than one of these regulations or rules, with virtually the only unifying factor being the network itself. In the early days, businesses approached compliance by considering only regulations that applied to their industry and by limiting their view to a device or a network segment. This approach is no longer valid in most instances. Only an overarching view of your entire network will serve to provide compliance today.

Getting a holistic view of the network can be extremely challenging, given that your network likely spans a variety of locations and sites. Many regulations require compliance not just for your infrastructure but for those of business partners as well. Still another consideration is the fact that regulations change and grow as IT capabilities do, making today's compliant technology quickly outdated.

A major challenge to having the bird's eye view that compliance demands is the network itself. Most of today's networks were built in response to an immediate demand, resulting in an often inefficient "patchwork" of disparate devices. While the network may carry traffic, the devices are not designed to communicate. This can make gathering coherent information challenging at best.

In this paper, we will broadly overview the major types of compliance required today. We will also consider an approach to compliance based on the network as a whole, rather than on specific devices or areas. Finally, we will show how Dell Networking Solutions built on the guiding principles of network optimization, agility, and openness, which allows you to leverage your existing infrastructure, while keeping costs low as you design your network to meet your business as well as regulatory compliance requirements.

The compliance landscape

The table below provides a quick look at some of the major compliance requirements today. It does not attempt to cover international regulations, nor are we looking at any of the specifications in detail; the purpose is rather to illustrate how any organization could be subject to several regulations at the same time.

Act	Description	Applicability
EU Data Protection Directive	Provides protection for individuals with regard to the processing of personal data and on the free movement of such data. The directive regulates the processing of personal data within the European Union, and is an important component of EU privacy and human rights law.	Overarching data protection law that applies to virtually any organization collecting or disseminating personal data.
Federal Information Security Management Act (FISMA)	Requirements for security controls to be in place when federally regulated information is stored. The act requires each federal agency to develop, document, and implement an agency-wide program to provide security for the information and information systems that support the operations and assets of the agency.	Agencies that produce, use, store or transmit information, , including those provided or managed by another agency, contractor, or other source
Gramm-Leachy Bliley Act (GLBA)	Confidentiality and integrity of personal financial information stored by financial institutions. Key rules under the Act include *The Financial Privacy Rule* which governs the collection and disclosure of customers' personal financial information by financial institutions. It also applies to companies, regardless of whether they are financial institutions, who receive such information. *The Safeguards Rule* requires all financial institutions to design, implement and maintain safeguards to protect customer information.	Financial institutions or other companies – such as credit reporting agencies, appraisers and mortgage brokers – that receives customers' personal financial information.
International Organization for Standardization (ISO)	An international standard-setting body composed of representatives from various national standards organizations. ISO produces a variety of standards and reports, such as ISO/IEC TR 17799:2000 Code of Practice for Information Security Management and the ISO/IEC 27002:2005 that establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization.	Varies by specification. Learn more at http://www.iso.org.
Health Insurance Portability and Accountability Act (HIPAA)	Legislation that includes requirements for the privacy and security of identifiable patient health information. Privacy covers all records whether paper or electronic and the Security focuses on electronic information.	All departments, including those of business partners and remote clinics, that produce, use, store or

		transmit patient health records.
Payment Card Industry – Data Security Standard (PCI-DSS)	Developed by the major credit card companies as a guideline to help organizations that process card payments prevent credit card fraud, hacking and various other security issues. A company processing, storing, or risk losing the ability to process credit card payments. Merchants and service providers must validate compliance with an audit by a PCI DSS Qualified Security Assessor (QSA) Company.	Any organization or department that processes credit cards for payment of services. This crosses all vertical industries.
Sarbanes-Oxley (SOX)	Developed by two U.S. congressmen, Senator Paul Sarbanes and Representative Michael Oxley, in 2002 to create significant and tighter personal responsibility of corporate top management for the accuracy of reported financial statements and ensure privacy and integrity of financial data in publicly traded corporations.	Any publicly traded corporation.
Control Objectives for Information and related Technology (**COBIT**)	COBIT is not a regulation; it is a set of practices (framework) for IT Governance and information technology (IT) management.	
National Institute of Standards and Technology (**NIST**)	NIST is not a regulation; it provides best practices standards on which compliance can be constructed.	
17 CFR (Code of Federal Regulations 240, 17a-4or 17b-4	Provides for the type and length of data retention and storage media requirements.	Broker/Dealer, Financial Services.
21 CFR (Code of Federal Regulations) Part II	FDA – security, integrity, auditability.	Pharmaceuticals and medical device manufacturers.
Family Educational Rights and Privacy Act of 1974 (FERPA)	FERPA provides postsecondary students the right to inspect their education records and establishes conditions concerning the disclosure of these records to third parties.	Higher education institutions and companies who employ workers.

Compliance and your business

Your business may be directly or indirectly subject to a variety of different regulations. In some situations, these regulations will be clear because compliance officers will demand records and reports on an annual or quarterly basis. In some situations, however, you may not even be aware that your business is subject to regulation. The Payment Card Industry Data Security Standard, or PCI-DSS, is such a regulation. This spec is not a law, but rather a very prescriptive set of requirements assembled by five of the major credit card brands. PCI does not proactively look for infractions. What it does, however, is respond to security breaches. Certain industries, such as healthcare, are required to adhere to PCI but often have not done so; in some cases, this is due to the mistaken belief that the healthcare specific HIPAA statute will cover PCI compliance as well. In fact, however, HIPAA is an example of a "goal-oriented" specification, where the result is examined and how an organization reaches that result can vary, rather than a "prescriptive" specification, like PCI, where certain network elements are required in certain places.

The number of compliance regulations and business verticals that are affected by them continues to grow every year. Compiling the information needed for compliance can be a major initiative on its own. And now the burden of maintaining and regularly reporting on compliance is falling not only on the compliance officer, but also the IT and security professionals that control the network. Current and future initiatives that these individuals will be involved in will include network security, differentiated access control, real-time compliance remediation and reporting, infrastructure compliance enforcement and management, storage and clawback of information stores.

This process requires that you collect data from a variety of different pieces of IT equipment throughout the network, collate that data, take action where appropriate report, push policy, and assemble data into the required format as dictated by the compliance organization. While many disparate infrastructure and security devices have a subset of these capabilities, they may not be designed to interoperate with others elements in the network. This issue is compounded by the fact that the entire process is prone to human error.

Getting started

Regardless of your industry, compliance with some regulation will almost certainly affect you. How best to demonstrate compliance while still conducting business as usual is a huge consideration, particularly given the amount of time required of your already stretched staff. At Dell, we recommend that you start with the network because it is the bedrock that all of your security and IT infrastructure runs upon. Like security and privacy mandates, the network permeates the entire organization, making it the most logical place to begin a holistic view of any compliance requirement.

A reliable networking solutions vendor can provide you with the best practices you need to comply with regulations while ensuring that your business is not bogged down by the activity. Specific elements to consider when looking at a networking solutions vendor include:

A combination of IT and compliance expertise

IT can literally make or break a compliance initiative; on the other hand, having a highly compliant network that doesn't serve your business requirements will not serve your needs either. It is vital to look for a solutions vendor that has high marks in both areas. Dell Networking Solutions can help you

get more than the devices you need; we can get you the solutions as well as the professional expertise that you need. Not only can Dell provide the solutions that ensure a compliant network, but Dell professionals can support you all the way from performing your security assessment into concept and deployment and ongoing streamlined management and reporting.

A secure and optimized network

Complex networks are difficult to manage, secure, control and operate. Most networks do not start out as complex or insecure, but over time they can evolve into being just that. And because of inherent complexity, the network may:

- Inadvertently be open to a potential security breach (i.e. PCI, HIPAA or Chinese Walls);
- Be impossible to manage, so deploying rule sets for new policies become nearly impossible;
- Not support real-time or historical reporting, which results in difficulties in storage, compliance reporting or clawback of records to demonstrate compliance to governing bodies.

Our networking solutions can streamline your complex, inefficient network and help turn it into a compliance-friendly network--from an infrastructure, security and storage perspective. This approach is integrated into your network architecture based on your specific requirements. Not only does Dell provide the solution that will meet your networking needs for today, we build your network to be forward compatible to support your future business and compliance requirements as they evolve.

Open standards

On paper, a single vendor solution can look compelling when you are considering compliance. You may assume that because a single vendor is being used, their products could easily support a simple, optimized and fully compliant network. Unfortunately, this is rarely the case. Most vendors that tout the "one stop shop" lock you in to a specific technology that does not interoperate with other vendor equipment. While this is great for the vendor, it usurps your ability to choose or chart your own strategy. With an open ecosystem and architecture, network complexity, vendor lock-in and inefficient networks are eliminated; and at the same time, you maintain control over your own strategy. Dell Networking Solutions' open, standards-based approach allows you to deploy a highly interoperable, virtualized architecture that is extensible and scalable and that will simplify monitoring and reporting, which eases the compliance burden while allowing you to conduct business on your terms.

Planning for the business ahead

Both the business environment as well as the compliance regulations that your business must satisfy will not remain static. It is important that the solution choices you make today also operate as an agile and flexible strategic platform for forward compatibility; a platform that can accommodate future IT and compliance regulations without causing major disruptions or technology switch outs. Dell Networking Solutions provide the flexibility and agility needed for today's dynamic business environment, We help you change the equation to ensure that your network supports the business ahead while also being "forward leaning" to satisfy the compliance regulations that you may be faced with in the future.

Summary

You can't consider the compliance landscape today without taking a long, hard look at how your network supports it. Major regulations may overlap and the complexity that has crept into the network makes it difficult to ensure compliance of all regulations at any given time across a distributed infrastructure. Compliance enforcement and reporting can leach away valuable staff time, and often does not ensure accuracy or fulfillment of requirements. And of course, the entire process takes place on the backdrop of keeping your network up and running and your business competitive.

Dell Networking Solutions has the expertise you need. Our approach in everything we do includes openness, agility, optimization and flexibility, all of which are paramount to helping our customers achieve their goals. And our approach to compliance is no different. We can supply a complete solution and the expertise you require to ensure your business is compliant with the regulations that affect it today, while being ready to take advantage of the opportunities to drive your business ahead tomorrow.

Make the most of your network – and your business – with Dell.