

INTRODUCTION

Creating a Sustainable Infrastructure

CHAPTER 1

Understand Your Risk Exposure, Then Manage It

CHAPTER 2

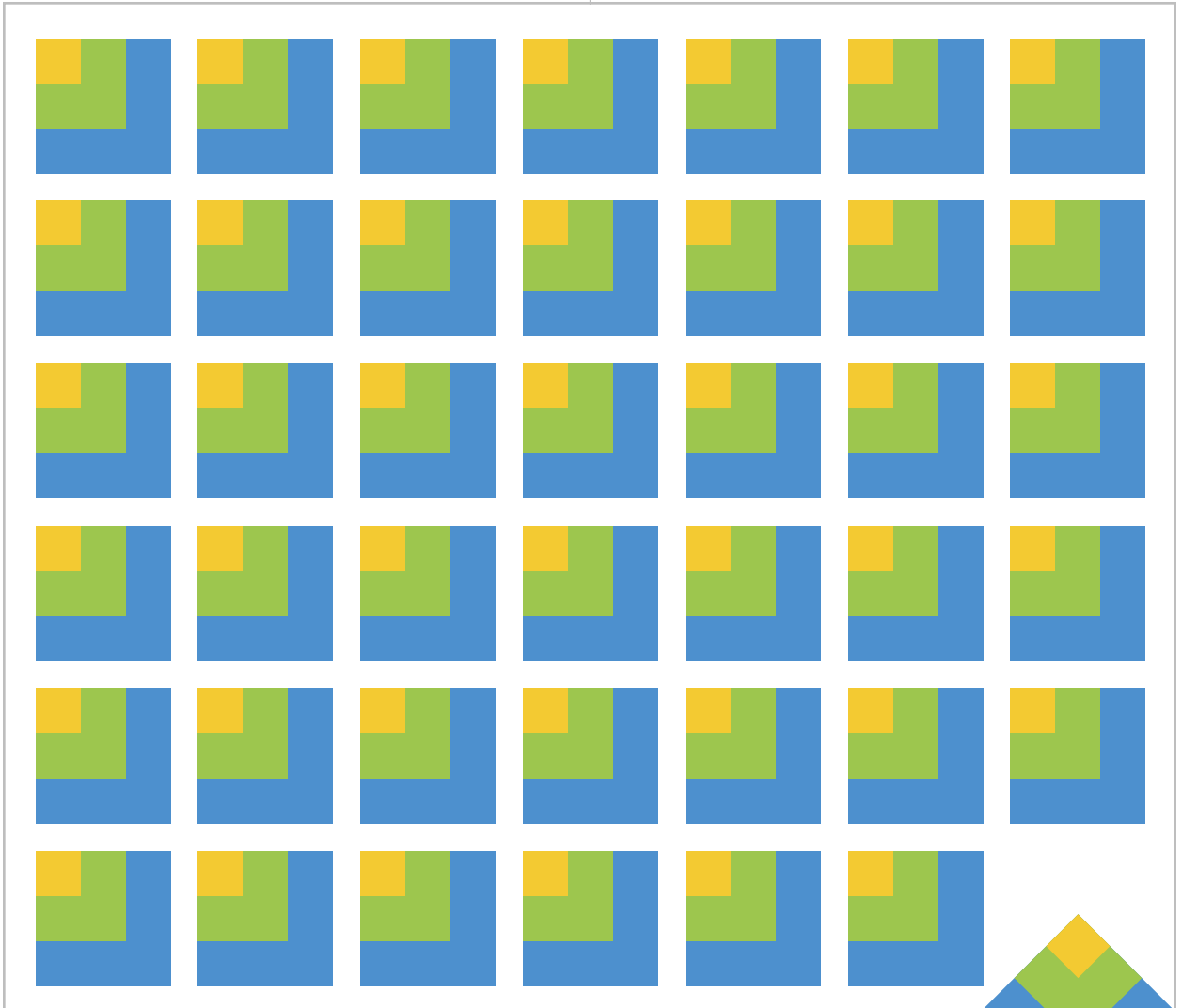
Bring Your Data Into Governance

CHAPTER 3

Extend Compliance Policies Across the Network

CHAPTER 4

Getting People on Board



Compliance 2.0

Compliance projects can bury your organization in process and paperwork. Creating a sustainable compliance operation starts with using risk management to prioritize and continues with understanding how to leverage new technology in your security, storage and networking infrastructure to create a true compliance infrastructure. BY ELISABETH HORWITT

Creating a Sustainable Infrastructure

INTRODUCTION

Creating a Sustainable Infrastructure

CHAPTER 1

Understand Your Risk Exposure, Then Manage It

CHAPTER 2

Bring Your Data Into Governance

CHAPTER 3

Extend Compliance Policies Across the Network

CHAPTER 4

Getting People on Board

WHEN REGULATIONS LIKE the Sarbanes-Oxley (SOX) and Health Insurance Portability and Accountability acts (HIPAA) came into full effect a few years ago, corporate IT and security managers found themselves scrambling to obey the letter of the law in every paragraph.

Regulators initially gave little help to businesses on how to prioritize compliance efforts: The general consensus was that you had to meet every SOX or HIPAA requirement, or at least make a good effort to do so.

Businesses have historically used a piecemeal approach to compliance, in which the medical equipment division concentrated on HIPAA, the financial group on SOX and each business group, subsidiary and division had its own security, data retention and backup systems and practices. Companies used a “check-the-box, point-solution approach, tackling each regulation independently,” says John Rostern, director, technology risk management at Jefferson Wells International Inc.

As a result, companies wasted a lot of money and time, often not getting the results they want, industry sources agree.

Older and wiser, IT professionals and their business-side counterparts have begun Compliance 2.0, a more mature approach to compliance marked by at least two features:

- **A more holistic approach to technology.** The tools needed to become compliant are a mixture of compliance-specific tools and general IT infrastructure, but in both cases they can generally be leveraged for more than just one compliance silo. Understanding how to leverage related IT projects, such as disaster recovery or WAN upgrades, is also key to the current crop of compliance deployments.
- **Quantitative tools to prioritize compliance.** Risk management is becoming a powerful way for organizations to make decisions on which areas of compliance to put the most effort into. Their quantitative nature also helps give the business/technology dialogue some meat.

In the long run, the goal of all this is to transform compliance from a costly project to a sustainable operation.

“If companies treat compliance as a

INTRODUCTION

Creating a Sustainable Infrastructure

CHAPTER 1

Understand Your Risk Exposure, Then Manage It

CHAPTER 2

Bring Your Data Into Governance

CHAPTER 3

Extend Compliance Policies Across the Network

CHAPTER 4

Getting People on Board

destination, they are less likely to get an effective process, which will kill efficiency, and they will get a lot less ROI," Rostern says. "There are so many regulations now, the only practical approach to compliance is top-down and risk-oriented."

More recently, both regulators and corporate security officers have recognized that the old approach is both impractical and unproductive. Regulators are cutting businesses some slack and providing some guidance on which aspects of regulations are more important than others. "They want you to focus compliance efforts on areas of most risk, rather than trying to address every possible foreseeable issue," says French Caldwell, a vice president at Gartner Inc. in Stamford, Conn.

Enterprises are moving towards a top-down approach that starts with risk assessment and prioritization, experts agree. Gartner has seen "a real uptick in enterprise risk management in the last few months, at least anecdotally," Caldwell says. He estimates that around 20% of large enterprises "are taking a really serious look at ERM."

Neal Kirschner, director of IT audit and risk management services at Eisner LLP in New York, says, "Businesses need to prioritize their compliance efforts, first measuring risk, and the tradeoffs of cost vs. exposure."

Major rating agencies like Standard & Poor's recently upped the ante by announcing that they will start includ-

ing a company's deployment of an enterprise risk management strategy in their evaluations.

Governance, risk management and compliance are increasingly being treated by C-level security and IT executives as a single acronym—GRC—describing the three key aspects of an overall corporate risk assessment and compliance infrastructure that does the following:

- Prioritizes compliance efforts on the basis of business goals, constraints and risk vs. cost assessments.
- Deploys a consistent set of policies and controls across the enterprise.
- Makes compliance practices and policies an intrinsic part of the corporate IT infrastructure.
- Utilizes information technology to monitor, enforce and automate policies and controls.
- Leverages compliance practices and controls to meet overlapping requirements from multiple regulations, in order to lower costs and ensure consistency.

The following four-part series explores how companies are building a holistic approach to tackling compliance, in key areas like data retention and e-discovery, security, backup and disaster recovery. We'll look at what strategies work, as well as what technologies and practices support compliance goals. ■



SYMANTEC IS

Automated enforcement of policies that secure and manage your information and infrastructure.

COMPLIANCE.

SYMANTEC.COM/EVERYWHERE

Confidence in a connected world.



symantec™

© 2009 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

Understand Your Risk Exposure, Then Manage It

INTRODUCTION

Creating a Sustainable Infrastructure

CHAPTER 1

Understand Your Risk Exposure, Then Manage It

CHAPTER 2

Bring Your Data Into Governance

CHAPTER 3

Extend Compliance Policies Across the Network

CHAPTER 4

Getting People on Board

In the initial panic over SOX, HIPAA and the rest, companies created a lot of compliance stovepipes that are becoming security nightmares. Avoiding such a situation requires a top-down, risk management-driven, holistic approach that leverages modern technologies and is bound together by broad policies.

WHEN MIKE MILLER came on board in 2004 as the first chief information security officer at Media General Inc. in Richmond, Va., he found a patchwork of point security solutions developed by different groups. This not only left gaps in the company's security defenses, he says, but it also used up a lot of manpower. "We had two security administrators who were mainly event log checkers and box watchers."

Miller replaced a haphazard set of security practices and policies with a holistic strategy: "A set of overarching policies, procedures, standards and practices" that apply across the media conglomerate's 25 sites and are closely aligned with business priorities and practices.

"We're not a bank, but our executives recognize that security maintenance, practice and functions are part of doing business now," Miller says.

Miller and his team also replaced the patchwork with an enterprise-wide security and data protection infrastructure based on several security and data retention applications from Symantec Corp.

"One solution that takes care of

everything is cheaper and easier than point solutions,” he says.

Count Miller among those IT managers who prefer the one-stop-shop approach. Other IT managers have taken a different approach, fashioning their own infrastructures from multiple vendors’ products but with a similar goal.

More and more corporate IT, business and security executives have recognized that addressing internal and regulatory security requirements piecemeal with point solutions just doesn’t cut it. They are moving towards a top-down approach to security that addresses both business and regulatory priorities in an integrated fashion. Among other things, this enables companies to leverage their IT resources (and budgets) more effectively, by addressing multiple security requirements with the same controls, practices and software tools.

Media General, for example, comes under several regulations: the Sarbanes-Oxley Act because it’s publicly held; Payment Card Industry (PCI) regulations because it accepts credit card payments; the Health Insurance Portability and Accountability Act because human resources handles employee health records. While each regulation has “subtle nuances” when it comes to compliance, the regulations all share some basic requirements, Miller says, like antivirus software and firewalls and multiple control layers to prevent end users—not to mention system administra-

tors—from breaking the rules.

Creating the infrastructure that enables a company to address its security requirements in a holistic fashion is no cakewalk, however. As

“One solution that takes care of everything is cheaper and easier than point solutions.”

—MIKE MILLER,
Chief information security officer, Media General Inc.

with other aspects of a holistic compliance program, it requires a great deal of up-front assessment and planning, from a number of different aspects:

■ **Where you are.** Unless it intends to rip everything out and start from scratch, a company needs to take stock of its security practices, policies and technologies, determining its assets as well as gaps and vulnerabilities. Security software vendors like Symantec Corp., IBM (Watchfire), CA Inc. and NetIQ Corp. provide agent-based vulnerability monitoring software that can scan individual servers and desktops for potential problems, like out-of-date security patches.

Companies like Qualys Inc. and Accume Partners provide security

INTRODUCTION

Creating a Sustainable Infrastructure

CHAPTER 1

Understand Your Risk Exposure, Then Manage It

CHAPTER 2

Bring Your Data Into Governance

CHAPTER 3

Extend Compliance Policies Across the Network

CHAPTER 4

Getting People on Board

scanning services that test for internal and external vulnerabilities.

- **Where you want to go.** Companies need to assess business and regulatory drivers and risk vs. cost factors to determine which security policies and practices should be applied to which areas.

- **Constraints and obstacles.** These can be financial, human (narrow-minded executives, resistant end users), or technical (a mixed bag of proprietary legacy systems).

- **How to get there.** Once a company has defined its security goals, it can define them as policies and controls, and last, but not least, determine what technology tools will be useful in monitoring and enforcing them.

First Advantage Corp., a Poway, Calif.-based company that performs a variety of legal and tax consulting services for clients, followed this game plan both in its overall security strategy and for individual security measures. It uses Qualys' vulnerability management service, which scans the corporate IT infrastructure, particularly "anything Internet-facing, and all SOX systems," says Isabelle Theisen, the business information provider's chief security officer (CSO). The service is keyed into First Advantage's overall risk management program, "so their security controls are matched to ours."

First Advantage took a different approach with encryption. After assessing the security demands of internal users and applications, as well as major customers and regulators, Theisen's group determined that it needed to install an enterprise encryption system that spanned storage backup, mobile and laptop devices, databases and Web-facing applications. "Once we knew what was needed, we started doing R&D, reading the white papers and talking to vendors," Theisen says.

PICKING YOUR TOOLS

The security market is awash in specialized software tools that address pretty much every aspect of security. Just about every business has deployed a battalion of defenses against outside attacks, including firewalls, intrusion detection, spam filters and antivirus software. In the last couple of years, however, it's become alarmingly clear that some of the biggest security threats come from inside—from careless, ignorant or malicious employees.

Tools that can help companies thwart such attacks include the following:

- **Data loss prevention (DLP) software** from companies like Symantec, IronPort and McAfee Inc. monitor computer systems and outgoing emails for keywords, numbers or character strings. When the software

INTRODUCTION

Creating a Sustainable Infrastructure

CHAPTER 1

Understand Your Risk Exposure, Then Manage It

CHAPTER 2

Bring Your Data Into Governance

CHAPTER 3

Extend Compliance Policies Across the Network

CHAPTER 4

Getting People on Board

INTRODUCTION

Creating a Sustainable Infrastructure

CHAPTER 1

Understand Your Risk Exposure, Then Manage It

CHAPTER 2

Bring Your Data Into Governance

CHAPTER 3

Extend Compliance Policies Across the Network

CHAPTER 4

Getting People on Board

catches something that breaks a rule—an email attachment containing a number string that matches a Social Security pattern, for example—it can block the transmission, or alert the user or the administrator.

While a survey by Osterman Research Inc. in November 2008 found that only 18% of companies currently have formal DLP solutions, 71% of respondents said they have established policies designed to prevent data loss. Twenty-five percent monitor outgoing content without blocking it.

■ **Event log monitoring products** are available from companies like LogLogic Inc., SenSage Inc., LogRhythm Inc. and GFI Software Ltd. and as a service from companies like SecureWorks Inc. and Qualys. Security information or event management systems—originally geared to aggregate security alerts—from vendors such as Check Point Software Technologies Ltd., Prism Microsystems Inc. and Novell Inc. are also morphing to provide more compliance-oriented features.

These applications aggregate and normalize the event logs residing on servers, network devices and other systems. Some also provide a degree of workflow to route the information to designated reviewers, important for PCI compliance. In general, these programs can provide the documentation that auditors need to prove that policies and practices were implemented and successful. This is an evolving

area, and users will want to assess the range of devices supported and report capabilities that each product offers against their own needs.

■ **Identity and access management (IAM) systems** use a directory to centralize the management of user access rights, avoiding the administrative nightmare of having a different set of passwords and IDs for each corporate system and service. Privileged access management tools from vendors like e-DMZ Security LLC and Cyber-Ark Software Ltd. address administrators and other users with special access privileges. In addition to monitoring administrators' activities and recording "who did what, when," they use temporary passwords to grant privileged access in a controlled, time-limited way.

Rather than deploy separate tool sets to counter outside and internal security threats, savvy CSOs and IT leaders are addressing both types as part of an integrated security infrastructure. This holistic approach enables companies to leverage human and technological resources in a far more effective way, particularly since many security systems and practices can do double duty. ID and access management systems, for example, can be used to track and control access to corporate data and services via the Web for internal employees, customers and partners.

First Advantage is using Symantec's

INTRODUCTION

Creating a Sustainable Infrastructure

CHAPTER 1

Understand Your Risk Exposure, Then Manage It

CHAPTER 2

Bring Your Data Into Governance

CHAPTER 3

Extend Compliance Policies Across the Network

CHAPTER 4

Getting People on Board

DLP tool both to monitor incoming and outgoing emails for noncompliant material and as an inventory management tool to discover where confidential and sensitive information is stored, Theisen says. “Knowing where the data is helps us close the gaps.”

Still, integrating all the security tools and controls into a truly holistic infrastructure can be challenging. Not surprisingly, many companies turn to a platform vendor or service provider to do it for them. Symantec, CA, IBM, McAfee and SecureWorks are among the companies that offer a variety of software security tools on a more or less integrated, centrally managed platform. Such offerings may include IAM, real-time monitoring of the corporate IT infrastructure and intrusion detection and prevention. Some products also offer guidance and best practices for defining and deploying controls for specific regulations.

For companies that can’t afford to purchase and maintain those platforms, vendors like SecureWorks, McAfee, Qualys and CA offer Software as a Service versions of at least some security products.

Such platforms offer the ability to audit and accord security events, as well as to document the measures a company takes to prevent and address them. Regulations like SOX and HIPAA specifically require firms to monitor or have an audit trail, an accurate record of security events like unsuccessful log-in attempts and the granting or removal of privileged access.

Media General, for example, uses Symantec’s security software suite, as well as NetBackup backup and recovery software from Symantec subsidiary Veritas. One reason the media conglomerate chose Symantec was the vendor’s centralized management

“Knowing where the data is helps us close the gaps.”

—ISABELLE THEISEN

*Chief security officer,
First Advantage Corp.*

and reporting features, which fit well with Media General’s holistic, policy-based security strategy, says Miller.

Another way to achieve a holistic security and compliance infrastructure is via outsourcing.

American National Bank in Gonzales, Texas, for example, turned over the management of its security infrastructure to SecureWorks.

“Our IT oversight committee felt we needed to expand our security strategy overall, but in an integrated fashion, with one vendor,” to meet both internal and regulatory security requirements, says Gene Stroman, the bank’s CIO. “From a compliance standpoint, we fall under GLBA and the Bank Secrecy Act, which deals with customer information privacy.”

Atlanta-based SecureWorks has the

INTRODUCTION

Creating a Sustainable Infrastructure

CHAPTER 1

Understand Your Risk Exposure, Then Manage It

CHAPTER 2

Bring Your Data Into Governance

CHAPTER 3

Extend Compliance Policies Across the Network

CHAPTER 4

Getting People on Board

resources to provide security functions that the bank can't afford to do in-house, Stroman says. The security outsourcing vendor provides around-the-clock monitoring and a level of expertise that the bank could not obtain without hiring an in-house security expert.

SecureWorks' intrusion detection and prevention service monitors incoming and outgoing transmissions, as well as the event logs of key systems. Servers designated as security-critical are monitored in real time.

When something suspicious or out of the ordinary occurs, American National Bank's security people receive alerts of different levels depending on the nature of the event. For example, someone changing a port on a Web server or a file system filling up might be reported as information, for which no action need be taken; someone repeatedly attempting to log in as an administrator would set off a series of escalating warnings.

Not that the bank has completely turned its security over to its outsourcing vendor. It has its own security people, and clearly defined internal security policies that have been fully explained to SecureWorks' people. Those solid internal controls and the second layer of oversight provide checks and balances that are crucial to the success of the outsourcing relationship, Stroman explains. "Otherwise SecureWorks might see someone breaking into a system and assume it's normal internal behavior."

The bottom line: American National Bank now has a holistic security and compliance infrastructure, which enables it to effectively meet both internal security requirements and those set by regulators, Stroman says.

Compliance is having a profound effect on security-oriented software.

While other service providers and software vendors could have offered roughly the same functions, they would have had to use third-party offerings, "and we would have had four, five systems to maintain and keep information correlated across," Stroman says. "With SecureWorks, the firewall, IPS, internal log monitoring are all part of one system, and we can see all events in one place."

Compliance is having a profound effect on security-oriented software. One prominent log-management vendor reports that compliance budgets are fueling 70% of sales, even if only 30% of use. With such an impact, expect several categories of security software to continue to morph in the direction of compliance. The decision to either go with a single suite, integrate point tools or use a service provider will continue to be a dynamic process for several years to come. ■



RAPID7

UNIFIED VULNERABILITY MANAGEMENT

The Broadest Solution:

- Database
- Network/OS
- Web App
- Web 2.0

The only broad scanning solution that has deep database support.

Database Challenges:

- DB Configuration Issues
- Policy Violations
- Privilege Escalation
- Security Patches

Database Audits:

- Security vulnerabilities
- Configuration vulnerabilities
- Operational vulnerabilities

www.rapid7.com - 866-7RAPID7

Bring Your Data Into Governance

INTRODUCTION

Creating a Sustainable Infrastructure

CHAPTER 1

Understand Your Risk Exposure, Then Manage It

CHAPTER 2

Bring Your Data Into Governance

CHAPTER 3

Extend Compliance Policies Across the Network

CHAPTER 4

Getting People on Board

At its heart, compliance is about which data needs what protection. The holistic approach starts with classification and ends with a flexible storage infrastructure that leverages modern backup technologies.

DESPITE THE WELL-publicized penalties of being found in noncompliance with federal data retention and e-discovery rules, a great many companies don't have a data protection and retention infrastructure geared for compliance. Many, for example, are still storing email on Microsoft Exchange servers

A recent poll of in-house lawyers and executives found that 30% of companies have no archiving policies for preserving evidence for litigation discovery.

and backing up critical data on tape without additional facilities for retrieving data quickly or ensuring that it's kept for the right amount of time.

Even lawyers are culpable. A recent Deloitte Financial Advisory Services LLP poll of in-house lawyers and executives found that 30% of companies

have no archiving policies for preserving evidence for litigation discovery. Not surprisingly, a large percentage of U.S. corporations don't have them either, the study found.

It's not that corporate executives are unaware of a need for archiving, particularly of email. In a recent Barracuda Networks Inc. survey of 200 North American IT professionals, nearly 82% of respondents said email archiving is "important" or "very important" for their organizations.

What's missing is an overall data governance strategy, industry experts agree. *Data governance* is a catch-all term covering technologies and practices that let a business effectively leverage its data resources. Governance, risk management and compliance (GRC) are the three main ingredients of a holistic infrastructure that addresses business and regulatory requirements in an integrated fashion.

Indeed, one of the major obstacles to leveraging data governance in a holistic compliance infrastructure is lack of coordination among different corporate IT initiatives, says John Rostern, director of technology risk management at Jefferson Wells International Inc., which provides asset management, auditing and risk management services. Data governance concepts like master data management (MDM), which "introduce new ways of looking at things often take place in a vacuum, becoming point solutions instead of part of an integrated approach."

Many large enterprises are deploying MDM to get a better handle on customer-related data, but if the project team "lacks a chief security officer perspective, which would include archiving, retention, confidentiality, availability, integrity and disposal,"

Data governance is a catch-all term covering technologies and practices that let a business effectively leverage its data resources.

a company can miss a golden opportunity to use MDM for regulatory compliance as well, Rostern says.

The same could be said about other IT projects. Many companies are building more robust disaster recovery (DR) plans, for obvious reasons. In their attempts to sort out what types of data are most important, they don't necessarily connect the dots to the compliance impact of that data. These are the sorts of connections CIOs will have to drive and compliance teams will have to make in order to achieve holistic compliance strategies and operations.

Still, forward-thinking chief security officers (CSOs) and IT leaders have been building their risk management

INTRODUCTION

Creating a Sustainable Infrastructure

CHAPTER 1

Understand Your Risk Exposure, Then Manage It

CHAPTER 2

Bring Your Data Into Governance

CHAPTER 3

Extend Compliance Policies Across the Network

CHAPTER 4

Getting People on Board

INTRODUCTION

Creating a Sustainable Infrastructure

CHAPTER 1

Understand Your Risk Exposure, Then Manage It

CHAPTER 2

Bring Your Data Into Governance

CHAPTER 3

Extend Compliance Policies Across the Network

CHAPTER 4

Getting People on Board

strategies around data governance concepts—data classification in particular. This involves dividing data objects into “bins,” or virtual groups, based on what user or application generated the data, how it is used, how often it is accessed and whether it contains sensitive or critical information. This, in turn, can help an organization determine which backup, retention and security policies, technologies and controls to apply in order to meet business and regulatory requirements.

Still, data classification projects in some companies are driven by more operational concerns: What performance level is required by users of the application that creates the data, how much operational downtime or data loss can be tolerated and similar metrics that might be summarized as service-level agreements. So the effort doesn’t always get connected to compliance requirements, even where data classification is under way. But ultimately, that would be beneficial.

“Increasingly, businesses have determined that you can’t protect data if you don’t know what it is worth,” The CDI Institute stated in its 2006 Corporate Data Governance Best Practices report. “Once the value of corporate data is determined, the enterprise needs to calculate the probability for risk in a business process. It is then possible to evaluate how much to spend to protect and manage it, as well as where invest-

ments should be made in adequate controls.”

First Advantage Corp. CSO Isabelle Theisen is working with the Poway, Calif.-based company’s compliance officer to implement a records reten-

“Increasingly, businesses have determined that you can’t protect data if you don’t know what it is worth.”

—THE CDI INSTITUTE

tion policy as part of an enterprise data classification scheme. “Classification will determine how long we store the data, and where,” she explains.

Data classification can also inform a tiered storage strategy. IT departments have a number of choices in primary storage along the price/performance continuum, ranging from inexpensive boxes full of individual Serial Advanced Technology Attachment disks to high-capacity, high-performance Fibre Channel arrays with sophisticated RAID protection and extensive data management and replication features. In recent years, they have made choices based largely on the capacity and performance requirements of the attached applica-

INTRODUCTION

Creating a Sustainable Infrastructure

CHAPTER 1

Understand Your Risk Exposure, Then Manage It

CHAPTER 2

Bring Your Data Into Governance

CHAPTER 3

Extend Compliance Policies Across the Network

CHAPTER 4

Getting People on Board

tions. But a fuller classification scheme that also took into account the retention requirements mandated by regulatory compliance would ultimately both save money and make compliance easier.

The same can be said about secondary storage. Tape is still a cost-effective, high-volume medium for backing up, but it will never be as nimble at restoral as disk-based backup. Decisions about which backup and archival storage technologies to use have to be informed by compliance-aware data classification efforts in order to properly assess the various tradeoffs presented by tape, disk-based backup, continuous data protection, single-instance storage, content-addressable storage and the other various flavors of data protection and retention.

UNSTRUCTURED DATA IS THE BIG PROBLEM

Before data can be classified, however, it has to be found and identified: no easy job, experts agree.

Most companies have fairly good control of their structured databases, says Craig Rhinehart, director of IBM's compliance and discovery group. The problem is the unstructured information that now makes up about 80% of corporate data: Word documents, Web images, spreadsheets, emails and attachments. "It's a digital haystack," Rhinehart says.

Identifying and classifying the entire

haystack is next to impossible, primarily because so much of it resides outside corporate servers, on users' local hard drives, external drives, flash drives and laptops.

For most companies, getting users to classify the documents they create is a hopeless task. Users generally lack the discipline and are often creating emails and short documents in as much time as it takes to classify them.

Official policies that tell users "don't share this kind of data, keep this proprietary and confidential" also have limited effectiveness, according to Theisen. "At the end of the day, I created the data and saved it on my hard drive, and it's up to me to do the right thing with it."

Nevertheless, data governance plays a crucial role in a compliance and risk management infrastructure—so project leaders pick their shots and prioritize.

"Since we are very decentralized and have many different types of business units, we concentrated first on identifying high-risk data: anything related to Sarbanes-Oxley, and information that belonged to our biggest customers," Theisen explains. Once that is accomplished, she says she plans to expand the program to include all types of data.

Still, getting a grip on the thousands of emails generated every day in an organization is a major undertaking. While most business leaders have recognized that email is "embedded

in business-critical processes,” many still haven’t gotten around to building an archiving, backup and recovery infrastructure that supports email as a business-critical application, says Scott Robinson, chief technology officer at Datalink Corp., a systems integrator that specializes in email archiving.

That’s changing, however, and not just because regulators and litigators are coming down hard on companies that can’t deliver two years’ worth of emails that include the word *deposition* in two weeks’ time. When Barracuda asked IT managers to cite the most important reason for archiving messages, only 29% said regulatory compliance. Twenty-one percent said it was enabling user access to archived email; and 15% cited enabling user access to older mail when quotas are in effect.

PICKING YOUR TOOLS

The good news is that vendors have stepped up to the plate with a slew of management and automation tools and platforms.

Archiving and e-discovery software from companies like Quest Software Inc., GFI Software Ltd., IBM, Symantec Corp., CA Inc., EMC Corp., Open Text Corp. and Hewlett-Packard Co. automatically captures, scans, indexes and stores incoming and outgoing emails according to predefined keywords. Some products can be programmed to automatically transfer data among

storage media.

Deduplication can be a critical preliminary step to email archiving, because it eliminates all those copies that users typically create of attachments as they forward emails and

When IT managers were asked to cite the most important reason for archiving messages, only 29% said regulatory compliance.

reply to various people.

Snapshot software automatically backs up files at different points in time, so they can be retrieved as they were at a particular date.

Data discovery and profiling tools from vendors like Symantec (Vontu) and Harte-Hanks Inc. (Trillium) can go through a company’s databases and, using predefined character and number strings, keywords and patterns, pinpoint the location of critical and sensitive data such as personal customer information and credit card records. Once an organization’s data has been identified and profiled, it can be classified and protected according to business and regulatory requirements.

INTRODUCTION

Creating a Sustainable Infrastructure

CHAPTER 1

Understand Your Risk Exposure, Then Manage It

CHAPTER 2

Bring Your Data Into Governance

CHAPTER 3

Extend Compliance Policies Across the Network

CHAPTER 4

Getting People on Board

INTRODUCTION

Creating a Sustainable Infrastructure

CHAPTER 1

Understand Your Risk Exposure, Then Manage It

CHAPTER 2

Bring Your Data Into Governance

CHAPTER 3

Extend Compliance Policies Across the Network

CHAPTER 4

Getting People on Board

Data discovery and profiling is also a key component of data loss prevention software that monitors outgoing transmissions for critical or sensitive material that shouldn't leave the premises.

Some tools are here and more are coming: What's needed is a holistic, policy-driven strategy to put the pieces together. This comes back to data classification, which remains a major challenge—particularly since data doesn't exist in a vacuum.

"You have to also understand the criticality of the applications that generated it," Datalink's Robinson points out, "and also interdependencies: A tier-two application may not be critical but feed into a critical application, so if the first application goes down, the second can't operate."

It's also important to recognize that criticality levels change, Robinson notes, so organizations need some formal procedure for transferring data—particularly if it no longer needs to reside on top-tier storage that is expensive to maintain.

American National Bank has put in place an umbrella business continuity plan that classifies data as mission critical, critical or noncritical, for both security and disaster recovery, according to Gene Stroman, the bank's CIO.

Financial reports and document images are retained for three, five, seven years or indefinitely, depending on regulatory requirements. "It's all indexed by keyword, date and report

ID, so that customers, employees, litigators and auditors can get at it," Stroman says.

Mission-critical data is replicated in real time to off-site backup servers, "so if a server went down, we can fail over, no loss," Stroman says. Snapshots are taken of financial data at the end of the year and loaded into a SQL database, because "come January, the data is no longer valid and gets updated."

Current financial data is backed up to a network-attached storage (NAS) device, where it is easily accessible to the bank's end users if the primary system fails. At day's end, Symantec's NetBackup backs the data onto a tape drive. The NAS copy is then erased since the data becomes obsolete the following day.

DISASTER RECOVERY

BECOMING A COMPLIANCE ISSUE

While DR has traditionally been less a regulatory than a business issue for many industries, regulators are starting to take notice—particularly in the financial sector, says Jan W. Koster, director of technology risk management at systems integrator Accume Partners.

For several years, the Securities and Exchange Commission (SEC) has told large financial institutions that they need robust disaster recovery and continuity plans that will ensure continued operations during and after any disaster, from a pandemic that

Chapter 2: Bring Your Data Into Governance

decimates bank personnel to a terrorist attack that knocks out the stock exchange.

Many banks still keep their business continuity plans in paper form, in a big binder. This makes it difficult to update documents when, for example, new branches are added. Regulators are pressuring banks to store their plans electronically, so they can be accessed and updated online.

“Regulators are looking at it from a customer perspective,” Koster says. “If a disaster wipes out a bank’s data center and it can’t recover in a timely fashion, maybe customers can’t get their money out of an ATM machine.” The recent financial crisis should make regulators even more hard nosed, Koster says.

Business drivers and constraints, often more than regulatory requirements, are what should determine what measures a company takes and the human and monetary resources it expends on data retention, backup and recovery.

For example, Media General Inc. in Richmond, Va., comes under strict SEC regulations for archiving material that gets aired on its television stations, says Mike Miller, the media conglomerate’s chief information security officer. “Other than that, we’re mostly trying to get people to get rid of stuff. Folks in newsrooms have a tendency to keep everything in case they need it.” So material gets archived, “to make room on the production systems.”

Sometimes, the requirements of business users and customers can be more rigorous than those of federal regulators—and from a business point

“We’re mostly trying to get people to get rid of stuff. Folks in newsrooms have a tendency to keep everything.”

—MIKE MILLER,
Chief information security officer, Media General Inc.

of view, more important. Take the case of American National Bank, which is deploying a system that stores every general ledger, loan and financial report for the next 10 years, and makes them accessible to customers via the Web.

“No regulation requires us to keep those reports past two or three months,” Stroman says, “but we want to keep those transactions available to our customers and business users indefinitely.”

Whatever policy your company settles on, the key is to align the policies for disaster recovery and compliance with each other and with the technology strategy you employ for primary storage, backup, archive and restore. ■

INTRODUCTION

Creating a Sustainable Infrastructure

CHAPTER 1

Understand Your Risk Exposure, Then Manage It

CHAPTER 2

Bring Your Data Into Governance

CHAPTER 3

Extend Compliance Policies Across the Network

CHAPTER 4

Getting People on Board



Having Trouble Finding the Road to Policy Compliance?

Shavlik Technologies eliminates the detours and roadblocks to meeting your compliance objectives!

PCI, SOX, HIPAA, GLBA - These aren't just letters to you. They are mandates that drive how you secure the systems on your network. The road to achieving compliance mandates is not always clear. Shavlik provides the most direct route to achieving, proving, and sustaining compliance with internal mandates as well as external regulations. We will help you effectively navigate the route to policy conformance so you: 1) fix the gaps in your security and compliance status; 2) keep up with emerging regulations; 3) meet your compliance objectives; 4) lower your operational costs; and 5) reduce your risk of exposure. Most importantly in today's economy, we make it possible for you to build a more secure and compliant network while spending less time, less money, and less IT staff. Discover more about Shavlik - visit www.shavlik.com, email us at sales@shavlik.com, or call (800) 690-6911

Extend Policies Across the Network

INTRODUCTION

Creating a Sustainable Infrastructure

CHAPTER 1

Understand Your Risk Exposure, Then Manage It

CHAPTER 2

Bring Your Data Into Governance

CHAPTER 3

Extend Compliance Policies Across the Network

CHAPTER 4

Getting People on Board

Globalization, partnerships, distributed computing—all of these mean that compliance solutions have to work across networks. Enforcing policies means leveraging existing network security apparatus, but it can also mean optimizing your WAN to bring more control back to centralized data centers.

REGULATIONS LIKE THE Payment Card Industry Data Security Standard and the Sarbanes-Oxley (SOX) and Health Insurance Portability and Accountability acts (HIPAA) don't stop at the firewall, any more than business transactions do. Critical and sensitive information that the company owns and for which it is responsible increasingly resides at remote corporate sites, and on the systems of business partners, suppliers, customers and outsourcing vendors. IT and information security leaders are thus confronted with the challenge of enforcing compliance rules on systems, and in locations where their oversight and control is tenuous at best.

Take the case of Louisiana Rural Hospital Coalition (LRHC). Hurricane Katrina left Louisiana with only one level-one trauma hospital that serves both insured and uninsured customers. As a result, that hospital has been operating at 110% capacity for several years. LRHC came up with a solution: a Web-based telemedicine system that lets specialists at the trauma hospital share their expertise and collaborate on cases with rural physicians.

The system has become a "life-

INTRODUCTION

Creating a Sustainable Infrastructure

CHAPTER 1

Understand Your Risk Exposure, Then Manage It

CHAPTER 2

Bring Your Data Into Governance

CHAPTER 3

Extend Compliance Policies Across the Network

CHAPTER 4

Getting People on Board

altering solution” that provides specialized treatment and expertise to rural populations in Louisiana, says Jamie Welch, the coalition’s CIO. Before it could go operational, however, her team had to find a way to control and secure access to the records of some 1.5 million patients residing in 24 rural hospitals.

“We weren’t familiar with all the HIPAA regulations to start with,” Welch says. “We initially thought we could have all the hospitals just trust each other: Whatever’s there, you’re allowed to see. The compliance officer stepped in quick and said, ‘You can’t do that.’”

Ultimately, LRHC chose to leverage its existing network directory structure. Although it has a variety of them at different hospitals, LRHC was able to use an identity and access management (IAM) tool (in this case, from CA Inc.) to interface appropriately with all of them.

“We set up an infrastructure so that if a doctor at hospital A searches for *Welch*, and I’m at hospital B and not registered with his facility, he won’t see my name,” Welch says.

The platform also monitors and records activity on event logs and Web portals, and automatically sends alerts when it sees suspicious behavior.

“HIPAA requires that you be able to show who accessed what, when,” Welch says. “You need to be able to go back and say, ‘Jamie Welch logged in at this time, stayed on 10 minutes,

and looked at this ER and radiology report.’”

By automating the auditing, documentation and enforcement of security policies, Welch says she has been able to meet all of HIPAA’s requirements and get a clean audit.

COMPLIANCE OUTSIDE

THE FIREWALL

LRHC is hardly alone. The need to enforce federal regulations outside the central organization is changing the way companies are architecting and managing their networks, and has added a whole new level of difficulty to enforcing information security and retention policies.

Several recent trends have contributed to the increasingly distributed nature of business organizations, computing operations and data.

Globalization and the need for businesses to be physically close to customers have caused branch offices to proliferate around the world. Many such sites lack a local IT administrator, so security and backup duties fall on a busy office manager or the employees themselves.

Mergers and acquisitions have saddled many companies with semi-autonomous business units that are accustomed—and resistant—to giving up their own policies, practices, systems and local IT organizations.

Companies are creating electronic ties with customers, suppliers and business partners via Web-based por-

tals, Software as a Service and Web 2.0 applications like wikis and RSS feeds. In a July 2008 survey of 1,446 business executives, McKinsey & Co. found that 73% were using Web 2.0 technologies to improve customer

Security and IT leaders need to address three key points of access: remote systems, internal systems and the network itself.

service; 71% to acquire new customers in existing markets; and 53% to get customer participation in product development. While these Web-based applications and connections can be a tremendous competitive advantage, they can also make a company vulnerable.

Meanwhile, budget-challenged IT departments are outsourcing IT operations and back-office applications to third-party service providers.

“The outsourcing vendor says, ‘Give me remote access so I can change and update things,’” says Jan W. Koster, director of technology risk management at systems integrator Accume Partners. “It makes things easier for the service provider, but it also opens up a door” that could potentially lead to security or compliance breaches.

None of the above scenarios will automatically lead to a security breach, or the loss of critical or sensitive data. However, regulators aren’t going to be satisfied with “Hopefully this won’t happen”—nor, of course, should corporate IT and information system security managers.

Rather than treat internal and external compliance as separate problems, forward-thinking companies are attempting to extend corporate controls and policies over the network and out to remote sites—whenever, and to the extent that it’s possible, that is. Security and IT leaders need to address three key points of access, and therefore vulnerability: remote systems, internal systems and the network itself.

THE DISTRIBUTED CHALLENGE

In the past few years, the increasingly distributed nature of business organizations has emerged as a major compliance issue, not to mention a serious threat to corporate security. A November 2008 Osterman Research Inc. survey found that 49% of 139 respondents are concerned or very concerned about enforcing Web usage and Web security policies for employees who work remotely—for example, ensuring that they do not visit undesirable websites or download malware via the Web.

Regulations increasingly hold companies responsible for ensuring that data is sufficiently protected when it’s

INTRODUCTION

Creating a Sustainable Infrastructure

CHAPTER 1

Understand Your Risk Exposure, Then Manage It

CHAPTER 2

Bring Your Data Into Governance

CHAPTER 3

Extend Compliance Policies Across the Network

CHAPTER 4

Getting People on Board

residing outside the corporate firewall.

One increasingly popular way to address this problem is re-centralization: Have remote employees back up all their data, even run all applications and services, at the corporate data center, where it remains under the control of the central IT staff. This not only makes it far easier for IT to enforce security, data retention and other regulatory requirements, but it can also bring major savings in office equipment and internal IT costs.

However, centralizing remote sites' IT operations creates its own challenges. Increasing the distance between end users and their applications and data can mean poor response time, more latency than some applications can tolerate and congested WAN connections or overburdened Web server farms.

Vendors like Blue Coat Systems Inc., Cisco Systems Inc., Citrix Systems Inc. and Riverbed Technology Inc. address this issue with a combination of WAN bandwidth optimization technologies such as quality of service, protocol optimization and compression. They are designed to make transmissions faster and more efficient, thereby ensuring consistent response time while conserving bandwidth over long-distance connections.

Even with WAN optimization tools, it's impractical to have larger and overseas sites depend on remote links for all their computing needs. Many sites will at least have to retain their servers. However, it can still be cost-

effective to send regular backups to a central (or perhaps regional) location over optimized virtual private network connections.

“You often have business practices built up over a number of years, which are difficult to change without radically altering the way businesses operate.”

—NEAL KIRSCHNER,
Director of IT audit and risk management services, Eisner LLP

On the human side, business users tend to resist giving up their local IT administrators and familiar policies and practices, and being dictated to by the corporate IT division. “You often have business practices built up over a number of years, which are difficult to change without radically altering the way businesses operate,” says Neal Kirschner, director of IT audit and risk management services at Eisner LLP, a New York-based auditing and compliance services firm.

That's why it's so important to bring key players from all of the affected groups into the planning process, to make sure they understand the busi-

INTRODUCTION

Creating a Sustainable Infrastructure

CHAPTER 1

Understand Your Risk Exposure, Then Manage It

CHAPTER 2

Bring Your Data Into Governance

CHAPTER 3

Extend Compliance Policies Across the Network

CHAPTER 4

Getting People on Board

ness drivers for the move and the policies and practices involved.

Be aware, too, that centralizing IT operations from remote sites can introduce as well as address security problems. Remote users must now interact with corporate systems in an intimate fashion, on a daily basis. For example, if a branch office employee goes to lunch and leaves the desktop on, a casual visitor or contractor could sit down and invade the company's server network.

Companies need to make sure remote users are trained in all the latest corporate security and business continuance policies and practices even—or especially—if they are doing all their computing at the corporate data center. Banks are required by the Gramm-Leach-Bliley Act (GLBA) to “document and be able to prove that branch office employees are trained and can respond to either a security incident or a disaster, based on policies,” says Gene Stroman, CIO at American National Bank in Gonzales, Texas.

In a 2008 Computing Technology Industry Association survey, 71% of respondents said mobile and remote employees have access to corporate data and networks, but only 39% said their organizations have implemented security awareness training and education for remote users. Of those organizations that had implemented such training, 92% said they believe the number of major security breaches had been reduced.

Kirschner says regular audits and unannounced spot checks of remote sites are also important.

Still, even with good training and regular audits, enforcing compliance policies over the network remains problematic, often requiring more time and effort than most IT staffs can afford. That's where technology can help.

AN END-TO-END SOLUTION

As companies move toward a more holistic approach to compliance, they are looking into how to extend policies and controls to remote sites in an integrated way, rather than treating remote networked compliance as a separate issue. Security and compliance management platforms from vendors like Symantec Corp., CA, IBM and Novell Inc. provide tools that can manage internal and external compliance in an integrated way, and specifically address networked compliance issues. Among the common tools provided are:

- **Multilayered ID and authentication to control remote user access to data center systems.** A number of IAM suites now include federated ID management tools that target companies that need to provide Web-based access to the employees or customers of a large number of business partners. Once a customer is authenticated on one partner's network, he is automatically authenti-

INTRODUCTION

Creating a Sustainable Infrastructure

CHAPTER 1

Understand Your Risk Exposure, Then Manage It

CHAPTER 2

Bring Your Data Into Governance

CHAPTER 3

Extend Compliance Policies Across the Network

CHAPTER 4

Getting People on Board

INTRODUCTION

Creating a Sustainable Infrastructure

CHAPTER 1

Understand Your Risk Exposure, Then Manage It

CHAPTER 2

Bring Your Data Into Governance

CHAPTER 3

Extend Compliance Policies Across the Network

CHAPTER 4

Getting People on Board

cated on the others, enabling him to jump back and forth among trusted partners' websites without logging on each time.

- **Encryption** to protect data in transit between remote sites and the corporate data center.
- **Data loss prevention tools** to monitor outgoing emails and other transmissions for keywords, numbers or character strings, and either block prohibited material or alert an administrator (or both).
- **Event log management software** to monitor system and network logs and Simple Network Management Protocol traps for suspicious behavior (see [“Understand Your Risk Exposure, Then Manage It”](#)).

An increasingly popular way to manage networked compliance is to outsource. Global service providers can provide data backup and around-the-clock security monitoring across hundreds of geographically distributed sites, far more efficiently and effectively than can most corporate IT organizations. Service providers can also provide specialized expertise to help companies deal with specific networked compliance issues.

However, outsourcing can also both solve and raise security issues, particularly when multiple vendors are involved.

Community Resource Federal Credit Union (CRFCU), a \$60 million, 20-employee organization, is in that situation. One third-party provider hosts

its member website, a second provides home banking and bill-paying services, while a third processes and stores the member database.

This setup raised two security and compliance issues, according to Dan Cole, the union's CFO. First, in accordance with GLBA and SOX the union must ensure that all of its third-party providers' security and compliance practices and controls meet all of the security requirements that the union itself must meet.

Fortunately, the American Institute of Certified Public Accountants has made this a lot easier by coming out with Statement on Auditing Standards (SAS) 70, a set of guidelines for certifying that an outsourcing provider has the right controls in place for protecting and securing customers' data and systems. If an outside auditor attests that a service provider is SAS 70-compliant, “you can be confident that your third-party core processing is secured, backed up, and so on,” Accume's Koster says.

Almost all of the credit union's service providers conduct annual SAS 70 compliance audits, Cole says. The exception is Paragon Services Inc., which hosts the website, “but they don't deal with our member data, so it's less critical,” Cole says.

The second security issue was how to secure the union's internal, peer-to-peer network. “If someone got into our DMZ and had an employee password, they could gain access to our member data,” Cole explains.

A small organization, CRFCU lacked the resources to manage the three-layered security infrastructure it needed, Cole says. So it hired Security as a Service provider SecureWorks Inc. to deploy and manage a holistic, multi-layered security system that includes a firewall, virus protection and intrusion detection/prevention.

Naturally, the union thoroughly vetted SecureWorks' own security infrastructure and regulatory compliance, Cole says. "We got testimonials from current customers, reviewed their financial history and their audit and compliance reports—SAS 70 in particular."

THE BOTTOM LINE

In today's harsh regulatory and financial climate, companies basically need to treat their business partners as part of their business when it comes to risk management—not just to satisfy regulators, but also to ensure their own survival.

And service providers are only one type of business with which companies may have close relationships—and security and compliance concerns.

"We monitor every vendor we have a significant relationship with," for stability and financial viability, says American National Bank's Stroman. "It ties back to risk assessment: We need to know where would we be if this vendor went out of business, or had a breach. Especially those we deem mission critical."

Still, companies have only limited control over the compliance measures taken by their business partners. That's why many firms, particularly in highly regulated industries, are limiting the relationships and information

In today's harsh regulatory and financial climate, companies basically need to treat their business partners as part of their business when it comes to risk management.

they share with other companies.

American National Bank, for instance, outsources its security to SecureWorks but has no other outsourcing relationship, Stroman says. "This helps us in compliance, and we don't have to keep auditing each firm that might have our customer data on file. And we simply don't share customer data with our partners."

Which only highlights the importance of aligning your networking strategy with other aspects of compliance: If you don't know the data you're shipping over the WAN contains regulated customer data, you can't adequately control it and you won't be in compliance. ■

INTRODUCTION

Creating a Sustainable Infrastructure

CHAPTER 1

Understand Your Risk Exposure, Then Manage It

CHAPTER 2

Bring Your Data Into Governance

CHAPTER 3

Extend Compliance Policies Across the Network

CHAPTER 4

Getting People on Board

Mitigate 92% of critical Microsoft vulnerabilities It's easy – eliminate admin rights with BeyondTrust



Increase Security, Reduce Cost

A review of all vulnerabilities documented in last year's Microsoft Security Bulletins shows that configuring users to operate without administrator rights can mitigate the effects of 92 percent of critical Microsoft vulnerabilities¹. This increased protection comes with the added benefit of a 24% decrease in IT labor cost per desktop². Achieve all this in one simple step — adopt a strategy of Least Privilege security with BeyondTrust.

Least Privilege Management

BeyondTrust enables enterprises to easily move beyond the need to trust users with administrator rights by elevating privileges for authorized applications, system tasks, and approved software and ActiveX installations without end user input, pop-ups or consent dialogues. Empower your network administrators to manage this security policy from within Microsoft Group Policy. Secure your Active Directory network today!

For a free pilot installation contact us at 1.603.610.4250 or visit www.beyondtrust.com.

¹ Obtain a copy of the free report at www.beyondtrust.com/mitigatevulnerabilities

² "New Report Shows 92 Percent of Critical Microsoft Vulnerabilities are Mitigated by Eliminating Admin Rights", February 3, 2009, <http://www.businesswire.com/news/home/20090203005227/en>

Getting People On Board

INTRODUCTION

Creating a Sustainable Infrastructure

CHAPTER 1

Understand Your Risk Exposure, Then Manage It

CHAPTER 2

Bring Your Data Into Governance

CHAPTER 3

Extend Compliance Policies Across the Network

CHAPTER 4

Getting People on Board

In the end, compliance projects can fail if IT managers don't pay proper attention to people and policy. It's not just about getting input—it's also about putting in the mechanisms and controls to ensure that people adhere to policies, and understanding when policies have to change.

AS FIRST ADVANTAGE CORP.'S new chief security officer, Isabelle Theisen had the task of building a risk management and compliance infrastructure from scratch. Before she did any building, or indeed planning, she did a lot of talking: to C-level executives, business group and IT managers, end users, partners and key customers as well. She did this for two reasons: first, to get key players behind the project and avoid resistance down the road. But at least as importantly, she needed these people's input, the critical knowledge they could give her about "the business, the current infrastructure, the people, the risks." She also hired an outside firm to do an ISO security benchmark.

Nine months later, she had a strategic plan for the Poway, Calif.-based company, "with the criteria clearly listed, and the requirements and constraints understood by everyone at all levels." As a result, "we don't have to pitch to the CEO or CFO every time we needed to acquire this tool, or this person, or implement this methodology," Theisen says.

The human factor can make or break a holistic compliance and risk management program. IT and busi-

Chapter 4: Getting People On Board

ness leaders and internal auditors can be valuable sources of information and support—or serious obstacles to a project’s success.

“I’ve been in companies where you spend all your time dealing with turf and political issues and don’t get things done,” Theisen says.

A holistic compliance program is founded on knowledge, which is used to formulate the policies that drive the controls that are incorporated into IT systems, and the practices people must follow to comply with regulatory requirements.

Designing an infrastructure that makes this happen can be a monumental task.

“I was a CIO before I was an auditor, and people and process questions far outweigh technology issues” when it comes to compliance and risk management, says John Rostern, director of technology risk management at Jefferson Wells International Inc.

Fortunately, help and guidance are available from a variety of sources. What works best for a given company depends on a number of factors, including its size, how many regulations it falls under, its in-house resources and expertise and, of course, financial constraints.

GUIDANCE FROM THE EXPERTS

Companies that are building a compliance infrastructure from scratch can hire experience and expertise from consultants and systems integrators.

A growing number of public accounting firms have IT risk management and compliance divisions. New York-based Eisner LLP, for example, does consulting work around governance, IT risk management, security and compliance.

“I’ve been in companies where you spend all your time dealing with turf and political issues and don’t get things done.”

—ISABELLE THEISEN

*Chief security officer,
First Advantage Corp.*

“We talk to IT leaders about what types of security and backup controls they want in place, and from there, what management practices are needed to meet their objectives,” says Neil Kirschner, the firm’s director of IT audit and risk management services.

Such firms can help a company create a top-down, holistic strategy and avoid the pitfalls of a piecemeal approach. Eisner’s consultants begin by helping clients prioritize compliance efforts on the basis of risk assessment and business goals, Kirschner says. “We talk to IT leaders about what controls they want to see in place to ensure systems are backed

INTRODUCTION

Creating a Sustainable Infrastructure

CHAPTER 1

Understand Your Risk Exposure, Then Manage It

CHAPTER 2

Bring Your Data Into Governance

CHAPTER 3

Extend Compliance Policies Across the Network

CHAPTER 4

Getting People on Board

up, access is appropriately restricted, users authenticated when they sign on. From there, we can see what management practices and methodologies are needed to meet those controls.”

In determining how to meet compliance objectives, Kirschner’s people always consider what is practical, given the organization’s resources—or lack of them: “That’s always an issue, particularly in today’s economic climate.”

Rostern says, “Standardizing policies and procedures is key, and where we find a lot of organizations deficient.” It lets a company efficiently manage and audit controls across the enterprise, instead of requiring separate audits and documentation for each division or business group. Even if each group has a different combination of IT systems, “the process for reviewing and approving entitlements can be the same,” Rostern explains.

Consultants can also suggest software and practices that can ease the whole implementation process and keep the project on track when the client is on its own. Jefferson Wells, for example, often recommends an enterprise governance, risk and compliance (GRC) platform, Rostern says. Such platforms, from vendors like OpenPages Inc., Paisley, Oracle Corp., CA Inc. and MetricStream Inc., use best practices and automated workflows to guide users through defining and deploying compliance controls and practices. Executive dashboards and reporting tools provide upper-level security employees and IT man-

agers with a top-down view of what’s going on.

GRC is still embryonic and amorphous, both as a platform and as a corporate strategy. It has yet to demonstrate that its benefits are

“Standardizing policies and procedures is key, and where we find a lot of organizations deficient.”

—**JOHN ROSTERN,**

*Director of technology risk management,
Jefferson Wells International Inc.*

always worth the cost and the hassle, many experts agree.

“If I talk to 10 people, I get 20 different answers for what they think GRC is, which I think, by definition, raises the question whether there really is a software package or a suite of software packages from one vendor that would allow you to solve all those problems,” John Hagerty, a vice president and research fellow at AMR Research Inc. in Boston, said in a recent SearchCompliance.com interview on the value of GRC software.

One of the key difficulties with enterprise GRC management is that to be truly effective, it needs to address risk, governance and compliance across three domains: IT systems;

INTRODUCTION

Creating a Sustainable Infrastructure

CHAPTER 1

Understand Your Risk Exposure, Then Manage It

CHAPTER 2

Bring Your Data Into Governance

CHAPTER 3

Extend Compliance Policies Across the Network

CHAPTER 4

Getting People on Board

Chapter 4: Getting People On Board

INTRODUCTION

Creating a Sustainable Infrastructure

CHAPTER 1

Understand Your Risk Exposure, Then Manage It

CHAPTER 2

Bring Your Data Into Governance

CHAPTER 3

Extend Compliance Policies Across the Network

CHAPTER 4

Getting People on Board

business operations, which includes meeting Occupational Safety and Health Administration and Environmental Protection Agency guidelines; and financial risks and compliance requirements. Business leaders face this challenge as they get serious about a holistic compliance strategy, particularly in the area of enterprise risk management, which takes a top-down approach to addressing risk across all three domains in a balanced and integrated fashion. This can be crucial in the event of a major disaster such as Hurricane Katrina, which wreaked damage across all three domains.

But it isn't easy, since it involves bringing together groups that typically don't talk to each other: IT, business managers, auditors. To make things more difficult, today's GRC platform market is highly fragmented.

Products typically address either IT, operations or financial management, but not all three, according to a June 2008 Gartner Inc. report, "Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms." "Instead of acquiring separate solutions for finance, IT and other business units, many enterprises are choosing to use a single EGRC platform and, when necessary, integrating the many point and functional solutions to satisfy specific GRC needs," the report states.

Still, today's GRC platforms have their uses, says French Caldwell, a vice president at Stamford, Conn.-based

Gartner. They provide automated monitoring of controls, to ensure that they are still in place and functioning correctly, "as compared to manual monitoring, which is both time-consuming and not very effective," he points out.

That's a crucial capability, given

"Instead of acquiring separate solutions for finance, IT and other business units, many enterprises are choosing to use a single EGRC platform."

—GARTNER INC.

people's unfortunate tendency to disable controls, according to Caldwell. For example, "Sally works closely with vendors and isn't supposed to access the invoice system, because it would be easy for her to invent fictitious vendors and pay herself," Caldwell says. "Standard ERP-based financial applications have segregation of duty controls; the problem is, they can be turned off without the company realizing."

Sometimes, the intent is not malicious: an employee turns off the control that prevents her supervisor from reviewing her work records, and acci-

dentally turns off the same control for several dozen other employees.

GRC platforms not only track but also record and document exactly what compliance measures have been taken when, and by whom. This is cru-

“You need to document the risk-assessment process and show which high-priority risk areas you focused on. If you can’t prove you did the assessment, as far as the auditor or regulator is concerned, you’re toast.”

—FRENCH CALDWELL,
Vice president, Gartner Inc

cial, given that regulators and auditors won’t be satisfied with a company just telling them what compliance measures it has to adopt. For example, while regulators don’t expect you to comply with every paragraph of the Sarbanes-Oxley or Health Insurance Portability and Accountability acts, “you need to document the risk-assessment process and show which high-priority risk areas you focused on,” Caldwell warns. “If you can’t prove you did the assessment, as far as the auditor or regulator is con-

cerned, you’re toast.”

Another key feature of GRC platforms is audit management. Through workflow, reporting and automated tracking and remediation of deficiencies, they help a company ensure that its corporate and departmental policies are aligned with compliance and risk management objectives, Caldwell says. “You can’t coordinate an enterprise approach to compliance on an Excel spreadsheet.”

GRC platforms aren’t the right solution for everybody. Large enterprises with extensive onboard expertise in compliance and risk management may consider them unnecessary. And smaller companies may find them too complex and expensive, although vendors are increasingly targeting mid-sized firms with Software as a Service and scaled-down versions.

BEST PRACTICE BLUEPRINTS

When it comes to actually deploying compliance policies and controls within the enterprise IT infrastructure, best practice frameworks like the IT Infrastructure Library (ITIL) and the Control Objectives for Information and related Technology (COBIT) can provide useful guidance, experts agree. The two are complementary, according to Caldwell: “COBIT lays out control objectives, like ensuring security, that you can map rules and regulations to, but while it tells what you should do, it doesn’t say how to do it. So ITIL comes into play with the

INTRODUCTION

Creating a Sustainable Infrastructure

CHAPTER 1

Understand Your Risk Exposure, Then Manage It

CHAPTER 2

Bring Your Data Into Governance

CHAPTER 3

Extend Compliance Policies Across the Network

CHAPTER 4

Getting People on Board

INTRODUCTION

Creating a Sustainable Infrastructure

CHAPTER 1

Understand Your Risk Exposure, Then Manage It

CHAPTER 2

Bring Your Data Into Governance

CHAPTER 3

Extend Compliance Policies Across the Network

CHAPTER 4

Getting People on Board

‘how,’ in the form of best practices.”

GRC platforms, as well as audit and consulting firms, frequently incorporate COBIT and ITIL practices in their risk management and compliance services.

With or without help from a GRC platform or outside firm, a company’s overall objective is to come up with a consistent set of policies and controls that can be applied across the entire enterprise.

THE HUMAN FACTOR

Risk management and compliance infrastructures typically combine policies that tell users what to do and what not to do, and technology-based controls that monitor user activity and possibly block prohibited behaviors.

“You need a combination of holistic, overarching policies, and ways to monitor and control” both systems and people, “particularly if, like us, you’re a distributed company,” says Mike Miller, chief information security officer at Media General Inc. in Richmond, Va. The company’s internal auditors do regular spot checks at different locations, to ensure that users are following corporate policies like backing up to a remote site.

Seventy-nine percent of respondents to a November 2008 Osterman Research Inc. survey have established corporate policies against downloading certain types of files, while 76% have deployed systems that will

actively block downloads of certain file types.

However, a holistic compliance infrastructure is more than just the sum of its controls and policies. It needs to be dynamic and flexible, able to respond to changing business goals and priorities, new regulations and

“You need a combination of holistic, overarching policies, and ways to monitor and control [systems and people].”

—MIKE MILLER,
Chief information security officer, Media General Inc.

technologies. Companies need to set up a formal process for auditing and assessing controls and practices on an ongoing basis and, when appropriate, changing them. And formal channels are needed to elicit and receive input from business users, not just during the initial design and deployment phases but also on an ongoing basis. Otherwise the infrastructure can become a straitjacket that hampers rather than supports business goals.

“One of our recommendations is to have an overall governance framework, which includes a steering committee comprised of the main stake-

holders in the firm,” Eisner’s Kirschner says. “They can look at what the priorities are, help set direction and approve policies.”

Sometimes it’s the end users down in the trenches who provide the crucial feedback. Take the case of Media General. One of Miller’s ongoing jobs is riding herd on employees who fall in love with a new technology without taking into account the possible security risks it poses.

His most recent challenge was Skype. A lot of employees have been asking for it—or worse, putting it in without asking. They didn’t understand that the peer-to-peer communications protocol constitutes a heavy security threat, enabling outsiders to bypass the firewall and invade the network, Miller explains. He responded in two ways: by programming the company’s intrusion detection system to send alerts when it found Skype, and programming the directory not to recognize the protocol: “So if someone installs it, it wouldn’t work on our network.”

Then some people from the TV news side said they wanted to use Skype to enable a laptop equipped with a webcam to send a streaming video of live news coverage. This would mean the station could do live news coverage with a single reporter, instead of spending thousands of dollars to send three people out in a news van, they explained. That sold Miller. “So now we’re trying to figure out a way to do it securely.”

In order to ensure that information

flows freely in both directions, Miller recommends setting up a centralized function—one high-profile person, one group—that people can go to with questions. “I think of my whole securi-

“One of our recommendations is to have an overall governance framework, which includes a steering committee comprised of the main stakeholders in the firm.”

—NEIL KIRSCHNER,
Director of IT audit and risk management services, Eisner LLP

ty group as internal consultants: We answer a lot of emails.”

In addition, Miller holds an annual policy and procedure review, to which IT and business people are invited. “Nowadays, it’s mostly updates, but it’s also an opportunity for business people to say, ‘You know, doing things this way is a real pain in the neck.’ Often it’s a matter of going from ‘must’ to ‘should,’ giving them a bit more leeway. Although sometimes it goes the other way, from ‘should’ to ‘must.’

“That’s the way it generally works here: It’s a constant negotiation.” ■

INTRODUCTION

Creating a Sustainable Infrastructure

CHAPTER 1

Understand Your Risk Exposure, Then Manage It

CHAPTER 2

Bring Your Data Into Governance

CHAPTER 3

Extend Compliance Policies Across the Network

CHAPTER 4

Getting People on Board



Let them
roam
lose laptops
surf
audit
cut budgets

who cares **You do!** Liberating your people and freeing up time and resources makes productive sense. Sophos security and data protection solutions deliver: Install, set and forget. Easy on your time, easy on your system and easy on your business, everything from Endpoint to Compliance, Email, Web and Encryption is covered and all accessed and controlled with refreshing simplicity.

Now, with security taken care of, you've got the rest of the day to do all the other things that can't wait.

See for yourself – [learn more about Sophos today.](#)

SOPHOS
simply secure



ABOUT THE AUTHOR:



Elisabeth Horwitt is a contributing writer based in Waban, Mass. She has covered business IT issues and technologies for the past 26 years, including nine years as a senior editor at *Computerworld*. Write to her at editor@searchcio-midmarket.com.

INTRODUCTION

Creating a Sustainable Infrastructure

CHAPTER 1

Understand Your Risk Exposure, Then Manage It

CHAPTER 2

Bring Your Data Into Governance

CHAPTER 3

Extend Compliance Policies Across the Network

CHAPTER 4

Getting People on Board



SearchCompliance.com

Compliance 2.0 is produced by CIO Decisions/IT Strategies Media, © 2009 by TechTarget.

Jacqueline Biscobing
Managing Editor

Linda Koury
Art Director

Elisabeth Horwitt
Contributing Writer

Mark Schlack
Vice President, Editorial

Anne McCrory
Editorial Director

Karen Guglielmo
Executive Editor

Kristen Caretta, Alex Howard
and **Rachel Lebeaux**
Associate Editors

Christina Torode and **Linda Tucci**
Senior News Writers

FOR SALES INQUIRIES

Stephanie Corby
Director of Product Management
scorby@techtarget.com
(781) 657-1589

BUSINESS STAFF

Andrew Briney
Senior Vice President/Group Publisher

Stephanie Corby
Director of Product Management

Christopher Baer and **Theron Shreve**
Product Managers

Katie Graybeal
Marketing Manager

Kelly Dillon
Product Performance Associate

From our sponsors



- ▶ [Top Ten Ways to Simplify Configuration Management and Compliance Auditing](#)



- ▶ [Enterprise Vulnerability Management—White Paper](#)
Discusses how to proactively identify and remediate network vulnerabilities to prevent the exploitation of network weaknesses.



- ▶ [Download the Managing Spend on Information Security and Audit for Better Results Report](#)



- ▶ [Eliminate Admin Rights—Learn more about BeyondTrust Privilege Manager](#)

SOPHOS

simply secure

- ▶ [Stopping data leakage: Making the most of your security budget](#)