Avoiding Information Overload:
A Logical Approach to Managing Endpoint Security and Compliance

Introduction

One of the greatest issues facing corporations of all sizes today is that of regulatory compliance. As if corporate security threats were not enough to deal with, regulations such as Sarbanes-Oxley, HIPAA, FFIEC, GLBA and PCI now have long checklists of mandated requirements that must be adhered to – and thoroughly documented – by information technology departments.

There are several key challenges in dealing with these compliance issues. The first is the knowledge required of the regulations themselves that must be acquired in order to know what policies and procedures need to be put in place to meet the appropriate requirements. Fortunately, there are common elements to many of the regulations that can serve as a starting point.

The second challenge is managing the data itself that is generated from the servers, workstations and removable devices across the organization's network. Without a centralized management system, collecting and reporting on the data is too time consuming and expensive…thus the reason many organizations fail to comply with regulatory requirements.

This white paper addresses the common requirements for many of the current US and international security and privacy regulations and propose a logical approach to managing the volumes of data required for proving compliance.

How Many Balls Can One Juggle? The Challenge for Midmarket IT Departments

Small to midsize enterprises face a unique challenge in that they often confront the same security and compliance issues as larger organizations, but have significantly fewer resources with which to deal with them. Where large corporations have dedicated IT security staff, midmarket companies are frequently reliant upon one or two information technology staff members who carry a wide range of job responsibilities.

The resource constraints of smaller organizations create a constant struggle of priorities between assuring system uptime and availability, and creating and managing the assessments, system policies, controls, and audits necessary to ensure regulatory compliance. Unfortunately, the security and compliance piece can sometimes take a back seat to other admin functions, leaving companies open to hefty penalties and fines if audited.

In order to adequately mitigate security risks and address regulatory compliance issues, small to midsize enterprises must find a way to manage system data in such a way that will enable small or outsourced IT departments to tackle security and compliance issues with fewer resources so that no one area must be sacrificed for the other.

Common Requirement: Risk Assessment

All security and privacy regulations – whether state, federal, or international - require organizations to have a risk assessment and management process in place. The first step, of course, is identifying what data is actually on the system and which of it needs to be protected. As an example, in Section 164.306(a)(1), Security Management Process, HIPAA requires that organizations:

- Identify all systems and applications that deal with electronic protected health information (EPHI)
- Accurately and thoroughly assess risks to the confidentiality, integrity, or availability of IPHI
- Assess adequacy of current controls
- Implement a risk management program

Too often, organizations try to tackle data security within the firewall by monitoring all activities on all files and applications. This creates information overload, making the data virtually meaningless to both the security officer as well as the auditor. It also puts a strain on the network, negatively impacting system performance and providing a deterrent to monitoring.

A better solution is to perform a scan/analysis of files, applications, devices and users on the network to *identify* and *prioritize* the protected information and potential threats to it. A thorough scan for inappropriate content, spyware, P2P file sharing, instant messaging applications and non-corporate removable devices is another step that can effectively help assess a company's security risks on a network's endpoints.

Common Requirement: Access Control

Once the information on a network's endpoints has been identified and prioritized, appropriate controls must be put in place for assigning access to that information. While the details in each regulation vary, the basic principles are the same.

The FFIEC Security Handbook requires financial organizations to have "effective rights management" and the PCI DSS, HIPAA and ISO 27002 all require organizations to have:

- Access granted based on a business "need to know"
- Prompt changes to privileges and access resulting from job changes
- Regular review and certification of access

- Monitoring of user activity

In order to ensure compliance with these regulations, it is imperative that organizations take the time to establish access policies for individuals and groups and then apply those controls to the data. Although this can be accomplished manually through the Windows operating system, using information security software that has policy management capabilities built-in makes this much easier to maintain as people come and go from the organization.

More importantly, such software often contains the ability to control access at a much more granular level such as by time of day or via particular device. For instance, it may be acceptable for members of an accounting group to access customer files during business hours, but not acceptable for them to download them onto a USB stick drive or access them from a remote location on the weekend.

Common Requirement: Real-Time Information Systems Safeguards

Another consistent requirement across multiple regulations is that the information system itself be monitored and secured. This not only ensures integrity of the data contained on the network but also provides an additional benefit to the midmarket IT administrator: real-time monitoring of system events, including registry changes, can provide alerts on potential security issues as well as possible system outages.

The PCI DSS specifically requires that systems be monitored in real time and protected against the activities of malicious hackers by using anti-malware programs, and that those programs are updated regularly with the latest definitions and signatures.

Producing Proof of Compliance: Centralized Management & Audit Reports

It's not enough to say your organization is in compliance with regulations such as PCI DSS, SOX, GLBA and other regulations. When the auditors show up, a corporation has to be able to prove compliance, and in the IT world, that means showing audit-trail reports.

As Matt Roedell, vice president of information security and infrastructure at TruMark Financial Credit Union, said, "You've got to be able to prove that, 'Hey, not anyone can walk out of here with our entire member database.'"[1]

Kevin Doyle, information security manager for Pennsylvania State Employee Credit Union, said he has also seen an increased need to prove compliance, especially in the past few years.

"We noticed that auditors were more knowledgeable and more serious about security, and the scrutinizing level had gone up," Doyle reported.[2]

The only way to run a true audit-trail report is to have a centralized log management system to ensure control over scattered data from the servers, workstations and removable devices across the network. It is for that very reason that auditors are prodding companies to consider technology solutions that enable them to centrally manage their data, said Trent Henry, senior analyst at Burton Group: "So we have one place that can keep the information and have proper IT controls over the data to make sure it's not tampered with or lost or accessed by people who shouldn't, and that those policies are enforced."[3]

At the very least, a centralized system should include event logs collected from the Windows operating systems on all of the endpoints with sensitive data needing to be monitored for security or auditing purposes. Reports should then be able to be generated showing client shapshots of each machine at given times, logon/logoff times by user, file and application access and usage, and any other system changes that would indicate a potential security breach. Reports should also be able to show that the appropriate file and application controls are in place, and how they are being monitored and secured against tampering.

Conclusion

A number of standards organizations have come up with guidelines for implementing a policy-based regulatory compliance and security framework, including International Standard Organization (ISO) 17799, British Standard 7799 and the IT Governance Institute's Control Objectives for Information and Related Technology (COBIT). Using these frameworks helps companies develop a set of best practice policies for meeting base requirements across multiple regulations. These common requirements include risk assessment, access control, real-time information systems safeguards, centralized management and audit reporting.

As midmarket companies become increasingly more proactive in addressing compliance concerns and worries of security breaches, Gartner analysts say this is also driving the market for security information and event management (SIEM) products. According to Gartner research, as quoted in an April 2008 SearchCIO-Midmarket.com article, there has been a steady growth in the SEIM market over the past three years, with 85% growth in 2005, followed by 52% and 30% growth in 2006 and 2007.[4]

One issue addressed in a 2007 Gartner market overview was the fact that many of the leaders in the SEIM market did not have real-time notifications and event management, or were too complicated to customize for a more realistic level of security alerts. In 2008, however, smaller vendors such as FutureSoft with products like DynaComm PointGuard have entered the market with offerings that provide broader coverage across multiple security and compliance requirements and can be customized to only alert or report on events that are critical to a particular organization or regulatory compliance need.

The bottom line is that small to midsize enterprises have realized they can't put off policy creation, log management and security event management any longer. Fortunately, this

comes at a time when SEIM products like DynaComm PointGuard are becoming available that are simpler to use, at an affordable price point, for them to be able to manage their security and compliance issues effectively within the limitations of their internal or outsourced IT departments.

About FutureSoft and DynaComm PointGuard

Founded in 1982, FutureSoft is an international software company focused on developing information security and connectivity solutions. With offices in Houston and the UK, the company's customers span the globe and include government agencies, educational institutions and corporations of all sizes within the banking, financial services, legal, healthcare, manufacturing, telecom and automotive industries. Over a million computers have been secured or connected using our software.

FutureSoft's Windows-based security technology helps organizations protect their most critical informational and IT assets from attack. The company's flagship product, DynaComm PointGuard, is designed to help small to mid-size enterprises increase productivity and reduce IT management and security costs through an integrated asset management and protection solution. Its centralized console enables administrators to get a total picture of user activity on all endpoints within the organization, while its granularity allows for both flexibility and control of sensitive data files, applications and devices on the network.

PointGuard provides endpoint security through spyware protection, insider threat assessment, data leak prevention, compliance auditing, policy creation and enforcement, USB/removable device management and real-time host-based monitoring. It also helps increase employee productivity by controlling application usage, and reduces costly system downtime through real-time system event monitoring.

For more information on FutureSoft and DynaComm PointGuard, visit www.futuresoft.com or call 1-800-989-8908.

FutureSoft is a Microsoft Gold Certified ISV Partner.

Footnotes

[1] *Compliance-burdened CIOs turning to security management tools*, by Zach Church Search CIO-Midmarket.com, April 8, 2008

[2] *Credit union takes top-down approach to compliance*, by Elisabeth Horwitt SearchSMB.com, May 16, 2006

[3] *Log management push has its roots in compliance*, by Marcia Savage

SearchSecurity.com, June 20, 2007

[4] *Compliance-burdened CIOs turning to security management tools*, by Zach Church Search CIO-Midmarket.com, April 8, 2008