



Data Security

The Role of ITAM in Regulatory Security Compliance

Finding a business that doesn't have some regulatory compliance challenge is rare these days. From Sarbanes-Oxley to Gramm-Leach-Bliley to HIPAA, regulatory compliance is a major ongoing issue for corporate America. In most regulatory scenarios, IT asset management plays a strategic role in compliance, and that role is expanding as organizations more closely align ITAM with security initiatives driven by compliance requirements.

Virtually all of the prominent regulatory mandates require companies to document that IT controls are in place to ensure the security of sensitive data. As a result of this compliance requirement, many companies are implementing security configuration management technologies and methodologies. A subset of system configuration management, security configuration management is a key enabler of compliance with most major regulatory mandates, ***and IT asset management is a key enabler of comprehensive security configuration management.***

The road to regulatory compliance can be a bumpy one, and for many organizations it can quickly become a Catch-22 situation. This is because most mandates provide only general guidance on what constitutes compliance and how to achieve it. Lacking from the mandates is concrete direction on what specific procedures, processes and internal controls are needed. Companies are left on their own to determine how they will comply. Fortunately, IT management best practices help to fill that gap by providing a framework for implementing the processes and IT controls necessary for compliance. By adhering to best practices, the path to compliance becomes much easier to navigate.

Security configuration management is a relatively new discipline that is receiving significant interest in light of the security requirements of regulatory mandates. One reason is that many regulatory measures specifically cite security configuration controls as necessary components of a security methodology required for compliance. Another reason is that, depending on the tools involved, security configuration management is now sufficiently automated to the point that it is a very cost-effective means of securing computers and the confidential information they maintain.

The rise of security configuration management is being driven in part by inherent limitations in the traditional network security paradigm – the defensive perimeter. Perimeter defenses incorporate a variety of tools and technologies including firewalls, anti-virus applications, identity authentication, intrusion detection, data encryption, vulnerability scanning and virtual private networks, among others. But perimeter defense remains a delicate balancing act that has to both restrict and allow access to information, systems and resources. An incorrect balance can lead to excessive exposure to vulnerability exploits or a backlash from end users unable to do their jobs because they can't access the IT resources they need. And perhaps just as important, perimeter defenses do little to protect against access to confidential information by those legitimately inside the perimeter. In fact, studies report that more than half of data security breaches are the result of malicious insider activity or end-user errors.

There are a variety of reasons for implementing IT asset management tools and processes, from optimizing asset utilization to lowering acquisition and maintenance costs to improving IT service delivery. But recently regulatory compliance has become a major driver of ITAM adoption. In the case of security configuration management, thorough asset knowledge is the foundation upon which IT builds its security configuration standards and controls. The first step in creating security configuration standards and controls is to know what you have in your IT environment. That begins with a comprehensive inventory of hardware and software IT assets in the organization. The reason for this is simple – before you can secure an asset (in this case a workstation, laptop or server), you first have to know that it exists in your environment. Then you have to determine its configuration state and its role in the IT environment and organization. With today's sophisticated hacker tools and attack vectors, it only takes one unsecured workstation or server to create a serious security hole in your network.

Most regulatory measures that seek to impose security controls begin with a thorough risk assessment step. The first phase is discovery – determining which assets need security controls according to the mandate. The next step is a comprehensive vulnerability scan to identify those systems which are not securely configured. Only then

can IT begin the work of securely configuring computer systems.

While a solid ITAM program has several data components, it is the configuration information of IT assets that is most important to security configuration management. Misconfigured systems are a primary source of security vulnerabilities. The Center for Internet Security (CIS) identifies six major types of system vulnerabilities, and all of them must be addressed when pursuing compliance:

- 1 Insecure accounts, such as null password or accounts with no password expiration,
- 2 Unnecessary Windows services like Telnet and Remote Access,
- 3 Backdoors, including Netbus, Backorifice, and Subseven,
- 4 Misconfigurations, including improperly configured permissions and null sessions,
- 5 Software defects, more commonly known as bugs and vulnerabilities, and
- 6 Spyware, which comes in many varieties.

Of these six vulnerability types, only software defects and spyware are addressed with dedicated IT tools (patch management and anti-spyware applications). The rest of the vulnerabilities are best addressed through security configuration management – that is, eliminating the vulnerabilities at the system level. With this in mind, it is easy to see why configuration data for each asset is so important. And it becomes even more vital when you consider that each computer can have hundreds of security related configuration settings. Multiply that by the hundreds or thousands of computers a typical company manages, and the complexity of the task becomes quite apparent.

Because of the sheer size of the effort, it is much easier and more effective to establish security configuration standards for the various types of computers based on their roles in the environment, and their relation to the security requirements of any particular regulatory measure. This is typically and most effectively accomplished by implementing and enforcing computer security policies, sets of access and configuration controls that determine who can do what with any given computer. The benefit of this approach is that several security standards bodies like the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) have standardized security policy templates based on consensus best practices recommendations. These templates are freely available, and with a minimum of modification can be adapted to the vast majority of IT environments.

With a complete database of configuration information in hand, the IT department can properly prioritize the assets and configuration remediation required to achieve security compliance. The ultimate goal is to align every relevant asset and its configuration with the security requirements set forth by the regulation. Of course, because compliance is an ongoing process, once the security configuration phase has been completed organizations still need to maintain compliance. Once again, ITAM can play a key role in that ongoing process by providing a mechanism to periodically validate security configurations, and to periodically discover new instances of non-compliance.

In many ways, compliance is a journey with definable steps but no final destination. Even when companies achieve compliance, they must continuously sustain it over time. It is up to each individual organization to develop its own compliance strategies and to implement the processes and controls that will satisfy auditors. But by leveraging ITAM and industry best practices as enablers, the path to compliance becomes much less complex and easier to manage.

Kim Pearson is CEO of New Boundary Technologies

