

Sarbanes-Oxley

COMPLIANCE JOURNAL

WWW.S-OX.COM

When Insider Threats Meet Sarbanes-Oxley

February 13, 2006

Many security practitioners divide security into three distinct but related areas: external threats, internal threats and compliance. While it is fashionable to say that security doesn't equal compliance, and compliance doesn't equal security, one must acknowledge that there is a tremendous amount of overlap between the two. This is certainly the case when considering Sarbanes-Oxley compliance and insider threats.

Insider threat and Sarbanes-Oxley share many of the same dire consequences: loss of intellectual property, compromised data, damaged or destroyed assets and severed communications, to name a few. Failure to protect sensitive data and meet regulatory requirements can destroy customer trust, spur government fines, damage stock prices and invite lawsuits.

The following article will educate readers on the real dangers of insider threats and detail the strong connection between insider threats and compliance with Sarbanes-Oxley. Organizations that take an integrated, common approach to Sarbanes-Oxley compliance and insider threats will achieve a stronger overall security posture and can better address both audit and security points.

What is Insider Threat?

These are attacks from within an organization, perpetrated by trusted employees, consultants, partners and/or temporary workers. These individuals may act independently out of pure malice or for financial gain. They may even commit their crimes in concert with outsiders such as competitors, identity thieves, and organized crime groups. In some organizations there may even be potential ties to terrorism and nation-state threats.

What Makes Insider Threat Different from External Threats?

For one thing, insider threats are more difficult to address than external threats. The individuals perpetrating the crime are co-workers and friends; this makes the enemy murky and forces those confronting the problem to examine their own value system. Moreover, because policies and procedures are often loosely followed, it is hard to know at what point a line has been crossed.

Insiders are often harder to detect than external criminals. This is sometimes attributed to a lack of organizational

adherence to best practices and an absence of defense-in-depth security strategies. While most organizations wouldn't even consider conducting business without security technologies such as firewalls, intrusion detection systems, anti-virus and virtual private networks (VPN), they sometimes stop there. As a result, they fail to secure and monitor assets that are the most mission critical such as mainframes and servers that process financial data, databases that store this data, legacy and proprietary applications that interact with it, network devices that transfer it and finally people that access and manipulate the data.

Monitoring these devices in real time, correlating the events and prioritizing them is of critical importance. Equally important are real-time and forensic investigation tools that help to detect and research issues and patterns. Visualization capabilities, reports, alerts, remediation and case management all need to be tightly integrated. Once the appropriate level of monitoring is in place, it becomes a tactical issue of aligning an organization's policies and process as well as regulatory compliance objectives into a cohesive solution that will address insider threat and Sarbanes-Oxley in tandem.

What is the Relationship between Insider Threat and Sarbanes-Oxley?

Having a well thought out Sarbanes-Oxley strategy can help achieve a stronger overall security posture, especially as it relates to insider threats. Once an organization understands this relationship, the security and compliance teams can be integrated in such a way that addresses both audit and security points.

Compliance is reached through documented, auditable and structured information protection. Specifically, the IT Governance Institute Control Objectives for Sarbanes-Oxley lists the following key points and I've included further explanation on how each point correlates to insider threat:

1. Use audit trails to track an incident

Insider threats require audit trails to determine who, when and how regardless of where in the company the information came from. Without this level of information insider threats are virtually impossible to detect. The days are long gone where security was a disparate, non-integrated group within an IT organization lacking executive support and the ability

to work across departments. When addressing insiders it is especially important to ensure that your business risks are being considered at the highest levels and include all applicable constituents.

2. Monitor and log security activity

Insider threats are all about internal system logs gathered from applications, servers, databases, etc. As with the first point, if the audit trails are not there, and you don't have supporting log information, you can't have a useful insider threat abatement policy. Insider logs can be voluminous and difficult to understand, especially when viewing them across a wide range of diverse products. But correlating the data against policies and standards that yield visuals and reports make this task manageable.

3. Review a sample of the incident reports to consider timeliness

Identification of the insider threat is the first step, but addressing it in a timely fashion is paramount. When issues arise there isn't time to invent new processes. The mechanism for allowing the right level of alerting, escalation and information sharing must be in place.

4. Review the problem management system

Ensure that threats are addressed inline with policy. This is especially true when it comes to making sure that only those that need access to information have it. Reports need to be generated to help those outside a response team understand the chain of events and track trends over time. The old saying—if you can't measure it then it doesn't exist—is especially true for security and compliance. Measurements and metrics help the solution evolve and improve over time.

5. Retain data capable of being reviewed, examined and reconstructed

Real-time data and reviews of the tracking mechanism are important. However, with insider threats, you also need access to accurate, secure, and holistic forensic data that will allow you to track activity well into the past. The discovery of a single insider threat can often later reveal a history of problems and multiple offenders.

Organizations are best served when taking a common approach to Sarbanes-Oxley compliance and insider threats. While one doesn't completely address the other, there are so many commonalities that it makes practical sense to combine the effort. By failing to do so, you may be putting your organization at even greater risk.

About Brian Contos, CISSP

Brian has over a decade of real-world security engineering and management expertise. As ArcSight's CSO he assists government organizations and Fortune 2000s with security strategy related to Enterprise Security Management solutions. Brian held security management and engineering positions at Riptech (an MSSP acquired by Symantec), Lucent Bell Labs, Compaq Computers and the Defense Information Systems Agency (DISA). He has worked and delivered presentations throughout the United States, South America, Western Europe and Asia and has written on security topics for several publications. Brian holds a B.S.B.A degree in Management Information Systems from the University of Arizona.



*Brian Contos
Chief Security Officer, ArcSight Inc.*



ArcSight, a leader in Enterprise Security Management (ESM), provides real-time threat management and compliance reporting yielding actionable insights into your security data. By comprehensively collecting, analyzing and managing security data, ArcSight ESM™ enables enterprises, government organizations and managed security service providers to centrally manage information risk more efficiently. ArcSight's customer base includes leading worldwide companies across many verticals—and more than 20 of the largest U.S. federal agencies.

For more information, visit: www.arcsight.com.