Sarbanes-Oxley: An Opportunity for Security Professionals
by Steven Drew - Monday, 06 December 2004.

Sarbanes-Oxley (SOX) is not just another regulation security professionals have to contend with in your already very busy lives. Instead, SOX should be viewed as opportunity for security teams to demonstrate your value as a key enabler of creating a sound business environment at the highest levels within your organizations. SOX presents this opportunity to every company, whether already a public entity that has to comply or private companies who fall outside mandated compliance, by providing a model for sound internal controls and a template to demonstrate the effectiveness those controls to executive management.

The first way SOX helps to demonstrate the importance of information security is that the regulation emphasizes the importance of your business critical systems. Executives typically think about sales, marketing and other revenue-centric business units when looking for ways to improve their business. However, they often overlook the critical systems that enable these units to effectively generate demand. SOX specifically points to these systems and raises the awareness of their criticality by making executives attest to the accuracy of their company's reported financial information. This attestation forces executives to ask questions regarding the activity on these systems and whether or not this activity could have altered the information they are receiving.

This leads to the second way SOX can help information security teams: creating an immediate need for security monitoring and reporting. All organizations need to implement technologies that monitor the activity on critical systems and be able to use this information to generate reports that illustrate this activity. Monitoring should be performed both at the network level using Intrusion Detection and/or Prevention Systems, as well as at the host level using log aggregation technologies that can gather security events from the appropriate log files. This information must then be consolidated to provide your team with a database of the security activity on critical network segments and information assets. With this information in hand, security teams can now easily generate reports showing the incidents targeting critical business systems and the actions taken to protect those hosts. Reports such as these can help security teams secure the funding they need to do their job by illustrating the threats facing the critical information assets and the effectiveness of the security program in thwarting these attacks. These reports can facilitate trust building between the executives and their security teams.

The last major way SOX can help security teams is by clearly justifying the need for more proactive security measures, such as vulnerability scanning and attaining threat intelligence. These measures will help you fortify your critical business systems from existing and emerging threats. Implementing robust scanning and intelligence programs will enable you to gain a better understanding of your assets' threat exposure level and provide this information to management along with the actual incidents and associated responses. Demonstrating effective proactive security measures will help build an additional layer of trust as executives see their security teams taking steps to reduce the likelihood of attacks against critical business systems, rather than merely maintaining a typical reactive policy.

All security teams should view the guidelines set forth by Sarbanes-Oxley as an opportunity. Implementing the controls and processes recommended by this Act will lead to a more secure business environment. More importantly, SOX raises executives' awareness of their critical business systems and the security surrounding these systems. This enables the security team to frequently demonstrate their value as a key enabler of business. This results in the executives gaining confidence in their security team, which will help future budgetary and personnel needs. Whether or not you have to comply with SOX, security teams should take a long look at this legislation and formulate a strategy to use it as a way to gain much needed visibility at the highest levels in the enterprise.

Steven Drew is Chief Operating Officer of LURHQ Corporation, a trusted provider of Managed Security Services. Founded in 1996, LURHQ protects the critical information assets of more than 400 customers by offering integrated Threat Management services.