FROM THE EDITOR-IN-CHIEF

Sarbanes–Oxley—a huge boon to information security in the US

Dr E. Eugene Schultz, Principal Computer Engineer, University of California-Berkeley Lab

Few pieces of legislation have affected so much so quickly and profoundly as the Sarbanes–Oxley (often abbreviated "SoX") Act of 2003. Triggered by accounting scandals such as Enron’s several years ago, SoX has many provisions, some of the most important of which require management of publicly traded companies to establish and maintain “an adequate internal control structure and procedures for financial reporting” as well as to provide an assessment of the effectiveness of the structure and procedures that have been established. As expected, accounting and legal firms have flourished as a result of SoX going into effect. Reports of large accounting firms searching desperately for additional SoX-qualified professionals have frequently made the news, especially recently because the compliance deadline date is rapidly approaching. What many, myself included, did not initially realize, however, was just how much SoX would impact the information security arena.

It is easy to understand how this Act would tap the knowledge and expertise of the audit community in which internal control is the central focus and well-established IT governance methodologies such as CoBIT are widely used. The relationship of SoX to the information security arena is not, however, quite as intuitive. For years information security professionals have struggled to vault their information security practices into positions of prominence and influence, ones that have strategic value to their organization. We’ve all tried a variety of approaches, some (such as establishing and using metrics as the basis of establishing value to an organization’s business) of which have worked considerably better than others. All things considered, however, it would be difficult to claim that a very large proportion of security practices today has achieved such a high and lofty status.

As staff within organizations tasked with achieving compliance with SoX studied the provisions of this Act, it became increasingly apparent that the adequacy of controls depends substantially on mainstream issues for information security professionals. Financial information, for example, resides on computing systems, storage devices and networks, all of which require suitable authentication and access control methods if one is to say with confidence that the data are reliable. File and directory integrity and auditability of accesses are also important considerations in data reliability, as is user authorization, specifically, tracing each user’s access to the systems, directories and files that hold financial data to explicit authorization by management. Ability to modify financial data and applications that process them and revocation of access for employees and contractors who have changed jobs or left an organization altogether are especially critical authorization issues. Information security has accumulated a large body of knowledge and technology that addresses all of these issues.

"The game is changing" for many information security professionals, therefore. Many Chief Information Security Officers (CISOs) who formerly had to use their very best personal and political skills to gain approval for addressing security-related concerns are finding their task easier—that they do not have to try as hard to "make the big sale" when interacting with senior management. What this seems to indicate is that all the tools we have in our proverbial arsenals, compliance rather than communicating risk-related concerns or...
trying to prove how security is an enabler or whatever else the approach may be the most effective.

The US commercial sector has long fought government regulation, but the severity of the fallout (particularly the public reaction) from the recent corporate accounting scandals in the US made legislation such as SoX inevitable. SoX calls for external auditors to render an opinion concerning the adequacy of controls, something that each company that must comply with SoX must soon face.

Numerous organizations are treating SoX as a purely financial matter, doing the very least they can do in response to this Act’s requirements and in some cases not even involving IT. Others, including part of the legal community, appear to just not get it. Furthermore, many organizations are not subject to the provisions of SoX. In these cases these organizations have not reaped the benefits that organizations that have wakened to the importance of information security in complying with SoX have. Perhaps even those who work for organizations falling outside of the scope of SoX and others who work for organizations that have not taken SoX very seriously may ultimately also benefit, however, as senior-level managers within organizations that must comply with SoX move on to other jobs. They are likely to take with them different attitudes towards information security and what it can do for their business’ “bottom line.” Only time will tell, but if I were a betting person, I’d place my bets on a widespread boost to the practice of information security as a whole.

Dr E. Eugene Schultz

E-mail address: eeugeneschultz2@aol.com

21 May 2004