

THE CHALLENGING ROLE OF A DIRECTOR

Susan Orr

Susan Orr Consulting

The role of a board member has grown in importance and complexity with the adoption of GLBA and Sarbanes Oxley. Corporate and IT governance obligations are now mandated and non compliance can carry stiff monetary penalties and prison sentences. To employ effective corporate and IT governance, there must be a clear understanding by the board of risk management, which entails identifying vulnerabilities and threats to information resources used in achieving business objectives, then deciding on the appropriate security and internal controls to mitigate the risks. Basically, the board has the ultimate responsibility for ensuring a secure physical and information systems environment; and ensuring the institution has protected itself from the inherent risks associated with the use of emerging technology and business processes in general. While this doesn't mean the board has to be involved in the day to day operations of the institution, it does need to oversee the development and implementation of appropriate and effective policies, procedures, and controls to ensure the security, confidentiality and integrity to customer's financial information.

Even though the risks institutions are faced with today really haven't changed; reputation, operational, strategic, liquidity, market, regulatory, and legal, the threats and vulnerabilities they are exposed to are growing more frequent, require less skill, and have increasingly more damaging payloads. High profile problems like system failures resulting from these threats and vulnerabilities or the lack of availability of systems due to a website hacking have elevated reputation risk to a place of greater importance. Reputation damage can be significant and culminate in a loss of customers, financial losses, or a negative impact on earnings and capital.

The concern over risks has also escalated among customers, stockholders, investors, and regulators, a like making security a top corporate priority, and no longer just a technology problem. Security is clearly a business issue and must begin in the board room. Risk management strategies must address the organization as a whole. Neither IT nor the board can operate in a vacuum. Risk mitigation strategies, which includes people, processes, and products must fit into overall corporate governance, and is a key factor in the alignment of IT to the overall business objectives.

For corporate governance to be truly effective, the board and executive management should implement some basic practices which start with establishing ownership for risk management and security at the board level and ensuring that business and IT management share the responsibility for IT security and it is integrated into the corporate security business objectives.

To properly implement IT governance, these four basic tenants need to be followed:

- Strategic alignment – to ensure security controls fit processes, that the security requirements are driven by corporate requirements, and that the investment in security is aligned with the overall strategy and risk profile of the institution.

- Value delivery – developing a set of security procedures that are based on best practices, are prioritized and communicated throughout the organization. The solutions must cover all business processes as well as IT.
- Risk management – there must be a clear understanding of risks by the board and executive management, an awareness of risk mitigation priorities, and an agreed upon risk profile.
- Performance measurement – there must be a well defined process for measuring progress and effectiveness of security controls and risk mitigation strategies.

In addition to the laws, regulations and increased dependence upon information systems, risk focused examinations have also amplified the need for understanding risk and implementing mitigation strategies, security, and internal controls. Too many institutions appear to inappropriately view governance and risk management as a compliance exercise evidenced by recent examination findings which cite lax board oversight, the lack of appropriate risk assessments, inadequate audit coverage, and weak security controls as the top deficiencies.

To successfully comply with regulatory mandates and pass examiner and auditor scrutiny the board of directors must implement an effective governance program and take the necessary steps to enhance risk management oversight by implementing a top down approach to securing corporate and information assets, or face the very real possibility of incurring regulatory enforcement actions, monetary penalties of up to \$1 million, and or up to 10 years in prison.

Susan Orr is a leading financial services expert with vast regulatory, risk management, and security best practice knowledge and expertise . During her 14 year tenure as a bank examiner, Susan held numerous lead positions including Regional IT Examination Specialist, Special Assistant to the Regional Director, Special Assistant to the Director of DSC, and Special Assistant to the Vice Chairman of the FDIC. Susan was also a lead instructor for the FDIC's technology school and was instrumental in key industry initiatives such as the FDIC E-Risk Strategic Initiatives Risk Monitoring Committee, the Chicago Region Interagency Technology Group, and the Federal Financial Institutions Examination Council (FFIEC) IT Handbook rewrites. Prior to launching her consulting practice, Susan was Vice President of Regulatory Compliance at for an Internet security company where she advised staff, customers, and partners on regulation, security, and risk management. Susan retains close relationships within the FFIEC agencies as well as industry trade groups to stay abreast on new technologies, best practices, and regulatory issues.

Susan currently consults for several security providers and vendors as well as performs IT security and regulatory reviews for financial institutions. She also speaks regularly at risk management and security educational seminars and has authored numerous white papers on emerging information technology and security risk management topics. Susan is a Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM) and Certified Risk Professional (CRP).