

IT: Growing Regulatory and Security Challenges

In a modern enterprise, IT is at the heart of all business activities: IT is responsible for the storage of critical data; IT forms the platform for business workflows; and, as firms such as Walmart have dramatically demonstrated, IT can be the source of tremendous competitive advantage. It was only a matter of time before state and federal legislators turned their attention to mandating the security, reliability and accuracy of business information generated and kept by corporate computing machinery. Legislative initiatives such as the Sarbanes Oxley Act of 2002 and the Health Insurance Portability Accountability Act (HIPAA) of 1996 have had a profound impact on business processes.

As businesses have experienced the effect of new information security laws, there has been a tendency to treat the extra effort associated with achieving compliance as a nuisance to be endured and an additional cost of doing business. However, a more productive and cost effective approach would be to re-think IT in terms of current and future regulatory initiatives. Businesses must learn to view their information technology investments as a regulated part of their enterprise, similar to accounting functions which routinely undergo required validation by outside financial auditors.

How Business Computing Has Changed

Client/server platforms came into businesses with little thought to regulatory or security matters. Companies deployed systems such as Netware 3.X to share expensive peripherals such as laser printers and to solve the "sneaker net" problem. Private corporate networks grew rapidly as the value-add became obvious, and remote access was a nominally secure service. Once the Internet became a public and widely available data transport and communications tool, companies adopted web applications with the same enthusiasm—and lack of concern for security and regulatory matters—as they did for the earlier closed, client/server networks.

Worms, viruses and other forms of malware became worrisome problems with the opening of desktops, home systems, and corporate networks to Internet access, and companies began to pay more serious attention to border and internal security. By the late 1990's, there were a variety of products offering countermeasures for malware and unwanted apps. Border security and challenge systems—firewalls, VPN, intrusion detection—became common, and many companies felt these safeguards were sufficient.

Regulation Hits Home

Several major events brought IT to the attention of government at both the state and federal levels:

- The collapse of Enron, leading to Sarbanes-Oxley
- 9/11 which led to heightened concerns about data security and disaster recovery
- The growth of identity theft which led to passage of the Identity Theft Penalty Enhancement Act of 2004
- Expansion of the 1994 Communications Assistance for Law Enforcement to include network infrastructure devices in libraries and colleges
- Digital Rights Management (DRM) technologies that seek to impose architectural changes in PC and other digital devices to assist the entertainment industry's IP enforcement efforts
- Two-factor authentication initiatives in the banking industry that also impacted banks' business partners—spurred by the Federal Financial Institutions Examination Council Guidance document on Internet banking authentication
- Health Insurance Portability & Accountability Act of 1996

Security and Regulation: An Almost Perfect Storm

Demands already placed on IT departments to protect networks against malware and intrusion has been made even greater by the addition of new regulatory requirements. As time passes, there are likely to be more, not fewer, security issues; and more, not fewer, regulatory initiatives. IT continues to move closer and closer to becoming a fully regulated corporate function. This requires a more holistic and strategic approach to IT planning, implementation, and maintenance with closer attention to regulatory compliance in all existing and proposed system deployments.

ABOUT THE AUTHOR: Dwayne Monroe has specialized in implementing network infrastructure and security solutions since 1994 for leading organizations such as Exelon; Wyeth Pharmaceuticals; Crown, Cork and Seal; Rohm & Haas; and the Uniform Code Council. As a Security Specialist with Anexinet's Infrastructure & Security Practice, Dwayne's work has focused on data security and the impact of political and regulatory trends on applied IT.



Anexinet Corporation
1040 First Avenue
Suite 108
King of Prussia, PA 19406 USA
Phone: 610-755-3400
Fax: 610-755-3420

ANEXINET.COM

Anexinet, an award-winning solutions integrator, applies leading-edge technology to complex business challenges, leading to simplified business processes, stronger IT organizations, and competitive advantages. Anexinet offers application development, integration, business intelligence, technology infrastructure, and enterprise program management (EPM) services to mid-size and Fortune 1000 companies and government agencies. Anexinet's experienced consultants ensure the success of clients' solutions through the company's Program Management Office (PMO) and a pragmatic approach that combines industry best practices experience with the company's innovative S.A.F.E-T2® software delivery model. Anexinet Near-Site® Development Centers enable project teams to design, develop and test client solutions within minutes of a client's location. Headquartered in Philadelphia, Anexinet has regional offices throughout the Delaware Valley and metropolitan New York City and Washington, D.C. areas.