Maintaining Security and Privacy Requires Getting “Back to Basics”

Richard O’Hanley

With the evolution of technology, we have seen the Extended Enterprise change into a new kind of organization known as the “Virtual Enterprise.” This is an organization that relies more heavily on the Internet to support a mobile workforce using handhelds to access vital data to conduct their daily business and to enable managers to stay connected and productive while traveling anywhere in the world. In addition, recent system attacks and viruses have exploited various technology vulnerabilities, causing organizations to spend considerable time and unbudgeted resources to contain and clean up their environments. Finally, the drive to reduce cost has forced a number of organizations to outsource or off-shore certain business functions and data management, forcing those organizations to address security and privacy issues with the third parties who maintain their outsourced infrastructure.

KEY CHALLENGES: TECHNOLOGY AND REGULATORY COMPLIANCE

Lost or stolen laptops used to top the list of events that kept information security managers awake at night. Today, however, handheld devices, which hold vital data, typically lack security controls and are more easily lost by their owners. Many organizations have been consolidating myriad systems into fewer, larger systems and aggregating data into more centralized databases in an effort to reduce costs. However, in the process, the risk to these organizations has increased, at least in the event that the systems or databases are compromised, or if the information moves across national borders in violation of regulatory requirements. In addition, due to inadequate design and testing, viruses and worms have continued to plague organizations by causing unscheduled downtime and unplanned costs as they exploit vulnerabilities in applications and operating systems. Lastly, the number of local and national regulations that impact organizations as they move to take advantage of new markets has been growing and shows no signs of slowing. The labyrinth of privacy regulations at the state, national, and international level has challenged many organizations that are trying to effectively comply with the requirements of these regulations, especially as they provide their organization’s data to third-party processors and move business functions off-shore. The technology and regulatory landscapes will change and evolve, but the basics for integrating security and privacy into an organization does
not change. These basics are Security Architecture, Risk Management, and Incident Response.

**SOLUTION: BACK TO BASICS**

The key to maintaining any security and privacy program relies on setting a clear, flexible strategy. Implementing that strategy will rely on key fundamentals that support the strategy, such as a defined security architecture, a risk management process and an incident response program that will address security and privacy for the organization regardless of the changes in technology or the regulatory landscape.

**FOCUS ON THE BASICS**

In this issue we are fortunate to have as guest editor Brian Geffert, CISA, CISM, CISSP, a Principal with Deloitte’s Security Services Practice. Brian and his colleagues at Deloitte have focused on security and privacy fundamentals. *Incorporating HIPAA Security Requirements into an Enterprise Security Program* outlines the steps to effectively and efficiently incorporating the HIPAA security requirements into your organization’s Enterprise Security Program and can be adapted for any regulation. *Document Theft: Appropriate Responses* discusses one organization’s response to an incident, while *Can You Handle the Headaches? Optimizing the Effectiveness of the Incident Management Process* provides approaches to improving your organization’s current incident management process. Finally, *Secure Coding: Building Security into the Software Development Life Cycle and Oracle Database Security* talk to the importance of considering security up-front and early in the development process to address vulnerabilities before deployment, and maintaining a security requirements baseline on a go-forward basis.

Technology and regulatory changes will always be a part of the business environment, and organizations will most likely be able to effectively and efficiently address these changes by simply focusing on the fundamentals.

Rich O’Hanley
Managing Editor