

CA Advisor

SECURITY MANAGEMENT NEWSLETTER

January 2009

CA Survey Finds Security Concerns Slow SOA/Web Service Implementation

By Lina Liberti

Despite the growing use of Service Oriented Architecture (SOA) and Web services by large corporations, security is still a major concern that is slowing their deployment, according to a new survey of senior IT executives sponsored by CA.



The [study](#) surveyed 555 IT executives from large and mid-size enterprises across the globe, regarding their views on SOA/Web services and security. One key finding was that 43 percent of the respondents felt that security was the most important issue surrounding the deployment of SOA/Web services applications, surpassing system performance (30 percent) and cost of ownership (29 percent).

Those concerns haven't stopped the organizations from implementing either SOA applications or Web services, however, with enterprises deploying SOA/Web services for a multitude of applications, from asset or project management to document management and CRM.

Furthermore, most of the organizations are providing at least some service access to external parties (68 percent of SOA and 75 percent of Web services), which increases critical security concerns. Given the security issues, 57 percent of those surveyed say that the further adoption of SOA/Web services by their organizations have been slowed.

Their concerns are validated by the fact that the SOA/Web services that these enterprises have implemented received several attacks in the last year, with some organizations reporting more than 20 such attacks in the past year.

The study found that depending on the number of SOA/Web services deployed, the surveyed organizations fit into one of four categories for the maturity of their security solutions. Companies just beginning to use these applications had the fewest amount of security measures in place. As organizations mature and they become more exposed, the number of security solutions also increases. But only about a quarter of the enterprises could be deemed advanced in their SOA/Web service security deployment.

In fact, the current state of SOA and Web services security is reminiscent of what happened with Web sites and portals about 10 years ago. As organizations rolled out Web applications, best-practice security systems and management approaches had not yet been resolved and

43% of survey respondents felt that security was the most important issue surrounding the deployment of SOA/Web services applications, surpassing system performance and cost of ownership.

security became a significant challenge to Web application and portal expansions. Once those challenges were overcome, Web application deployments flourished.

The Critical Importance of Security Integration

Notably, a greater percentage of IT executives from those advanced organizations (44 percent) rank security as one of the most critical issues regarding SOA/Web services than those who are the most exposed (37 percent). That may be because the more mature companies are already aware of the difficulties involved with providing sufficient security for their applications. One indication of that challenge is the broad range of security standards that the organizations of those surveyed have adopted or are planning to adopt within the next 12 months. These include Web services security (57 percent), XML encryption (45 percent), SOAP (37 percent) and REST (28 percent).

While the primary responsibility for SOA/Web services security once fell to service developers, that's no longer the case in most instances. More than 80 percent of surveyed organizations have IT security purchase and manage security solutions for service deployment. Not surprisingly, the IT execs surveyed see the importance of integrating SOA/Web services security with their companies' existing enterprise security systems and processes. Nearly all of the respondents (93 percent) answered that it is somewhat or highly critical that SOA/Web services security solutions be integrated with Identity and Access Management (IAM) systems. But only 43 percent of those surveyed say that their organizations have already implemented that integration, with 53 percent saying that integration will be completed within the next 12 months.

The study's findings suggest that the need for an organization's business teams to introduce more applications that are based on services will be balanced by the security readiness of the organization. The fact that respondents are deferring SOA and Web services applications for security reasons indicates a strong collaboration between business and IT security teams is beginning to happen. When this collaboration occurs, they are evaluating risk versus benefit to the business. By integrating the security systems and processes for services with the enterprise security systems that are already in place, principally IAM, the organization can increase the adoption of SOA/Web services while protecting itself against the risks associated with the services.

Lina Liberti brings 15 years of experience in the software and hardware industry with more than ten years of experience specifically in the security industry. At CA, Lina is vice president of product marketing for CA's Security Management business unit where she is responsible for defining the messaging, positioning, and go to market strategy for CA's identity and access management and security information management product lines.

Prior to joining CA, Lina was product line manager for emerging technologies at RSA where she oversaw product management and product marketing for RSA's single sign-on, smart card, and public key infrastructure (PKI) technologies. She also managed product management and product marketing at Memco before it was acquired by Platinum.

For the latest issue of CA Advisor: Security Management Newsletter, visit ca.com/newsletters/secure. To subscribe to receive future issues, or to manage your preferences, visit the [CA Preference Center](#).