Global report on SOA/Web services security initiatives.

AUTHORS:

Gib Trub, Managing Partner
Laurie Olski, Managing Director
GMG Insights

ADDITIONAL INPUT:

James McLeod-Warrick, President
Beacon Technology Partners

TOPIC:

SOA/Web services security solutions

PUBLICATION DATE:

September, 2008, version 1

Publishing Information

GMG Insights provides analysis, research and strategy services to companies with complex B2B sales. Publication headquarters, marketing and sales offices located at:

GMG Insights
95 Nason Hill Road
Sherborn, MA 01770
Phone: 508-545-1095
Fax: 866-725-7059
Internet: info@gmginsights.com

Methodology

This study focused on senior IT executives responsible for application development or IT security, with personal responsibility for developing, or managing others who develop, either SOA[i] or Web services[ii] applications; or responsibility for developing and implementing, or managing others who develop or implement IT security strategies and solutions. It included a worldwide quantitative survey with a confidence level of +/- 5%. The study was conducted in June 2008.

The quantitative analysis was conducted by Beacon Technology Partners, Maynard, MA. James McLeod-Warrick, President of Beacon Technology Partners, collaborated on the analysis and reporting of the findings.

This study was sponsored by CA.

Table of Contents

GMG Insights • 95 Nason Hill Road • Sherborn, MA 01770 P: 508-545-1095 | F: 866-725-7059

www.gmginsights.com

Synopsis

The introduction of Service Oriented Architecture[i] (SOA) and Web services[ii] has resulted in significant changes in how applications are developed and deployed. The development community and others are anxious to put these innovations to work immediately. At the same time, the implementation of SOA/Web services applications can open up a complex set of security and management issues. Once developed, SOA/Web services-based applications take on a life of their own. Without proper planning, organizations trying to secure those applications will find themselves in reactive mode, confronting risks and issues as they arise.

In the past, IT security was not often proactively involved in addressing security issues of new technologies. Many security solutions were implemented as an afterthought once risks were identified and understood – sometimes the hard way. SOA/Web services opens the "virtual door" of an organization to significant external risks. An after-the-fact approach to security will not sufficiently secure SOA/Web services implementations.

Senior IT executives seem to understand the importance of the security issue, 43% perceive security threats as the most critical issue relating to the implementation of SOA/Web services applications and 57% admit to slowing or deferring adoption of SOA/Web services due to security issues or concerns.

The threat appears to be real. SOA/Web services applications are already subject to targeted XML attacks. The potential risk is high; more than two-thirds of those surveyed have externally facing SOA and/or Web services applications.

In spite of the awareness of SOA/Web services security risks, just 25% of organizations can be considered mature in their adoption of appropriate security solutions. Even for those mature organizations, a significant investment in security solutions does not reduce their sense of risk, indicating a low comfort level with the security implications of these new development tools.

The vast majority of organizations with SOA/Web services implementations are still at risk, and most recognize it. They are putting some security solutions in place but few are doing so from the overarching perspective required for effective organizational security.

GMG Insights • 95 Nason Hill Road • Sherborn, MA 01770 P: 508-545-1095 | F: 866-725-7059

www.gmginsights.com

Implementation of SOA/Web services across a variety of categories

SOA and Web services represent a dramatic change in how applications are developed and deployed, and they are already being implemented across a wide spectrum of application categories in both mid-market ($100 to $999 million) and large enterprise ($1 billion+) organizations *(Figure 1 and 2).*

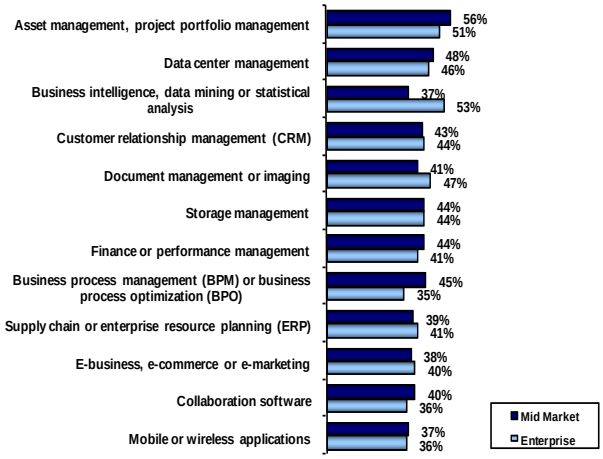


Figure 1: Implementation of SOA applications by mid-market and enterprise organizations, ranked by total.

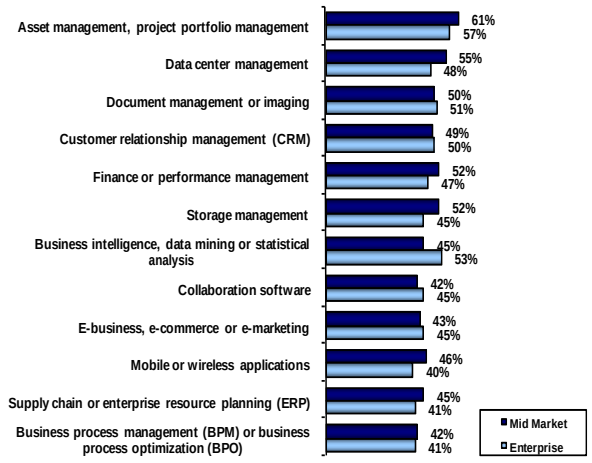


Figure 2: Implementation of Web services applications by mid-market and enterprise organizations, ranked by total.

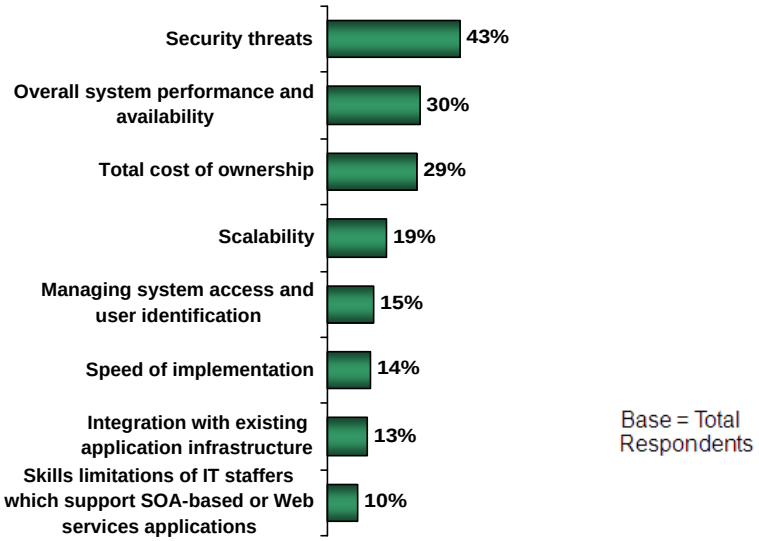
SOA/Web services implementations are being deployed across a wide variety of solution categories.

GMG Insights • 95 Nason Hill Road • Sherborn, MA 01770 P: 508-545-1095 | F: 866-725-7059

www.gmginsights.com

Security issues surrounding SOA/Web services have not been addressed

The significance of security issues surrounding SOA/Web services implementations is widely acknowledged: 43% of senior IT executives perceive security threats as the most critical issue relating to the implementation of SOA/Web services applications *(Figure 3).* This was true across all geographies surveyed and has impacted adoption rates across the globe.



43% of IT executives perceive security threats as the most critical issue relating to implementations of SOA/Web services applications.

Figure 3: Most critical issues perceived relating to SOA/Web services implementations.

In fact, 57% of senior IT executives admit to slowing or deferring adoption of SOA/Web services due to security issues or concerns. It is highly likely that the "promise" of SOA/Web services would be reached earlier if these security concerns were adequately addressed.

It seems senior IT executives have accurately perceived the criticality of security solutions for SOA/Web services. SOA/Web service applications are already subject to targeted XML attacks. Hackers are already well prepared to take advantage of the vulnerabilities that are exposed particularly when services are offered externally *(Figure 4).*

GMG Insights • 95 Nason Hill Road • Sherborn, MA 01770 P: 508-545-1095 | F: 866-725-7059

www.gmginsights.com

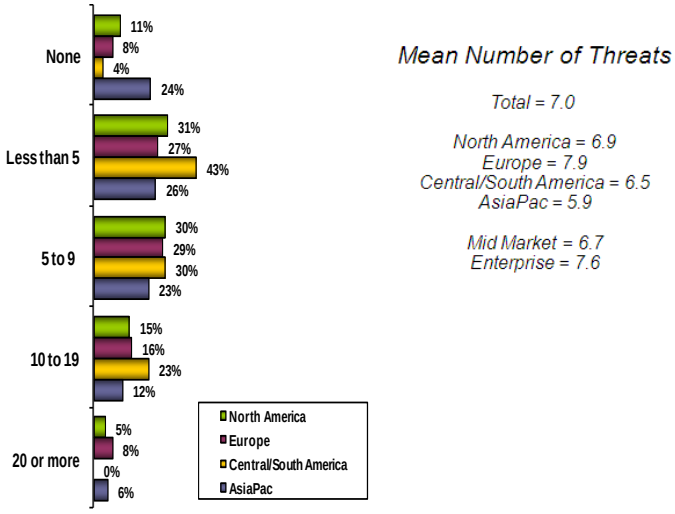


Figure 4: Number of XML targeted or other malware attacks against SOA/ Web services solutions in past year.

SOA/Web services solutions are already subject to XML targeted or other malware attacks.

Externally facing SOA/Web services implementations

In spite of the security concerns, organizations surveyed have a surprisingly high percent of externally facing SOA/Web services implementations *(Figure 5).*

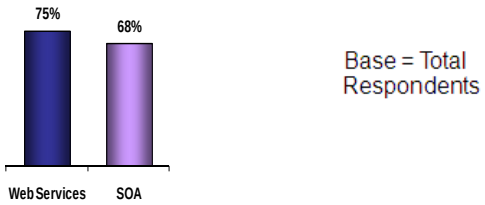


Figure 5: Externally facing SOA/Web services implementations.

Despite the security risks, external facing SOA/Web services implementations are common.

GMG Insights • 95 Nason Hill Road • Sherborn, MA 01770 P: 508-545-1095 | F: 866-725-7059

www.gmginsights.com

Given that SOA/Web services are designed for reuse, the concepts of "external" use and "internal" use have blurred so much they become meaningless. Security implementations for a service can not be based upon the presumption of internal use by trustworthy users. Organizations can anticipate that after deployment, usage of services will evolve. If it does not, the service itself is a failure. Every service implementation should be viewed as external and secured accordingly.

Identity and Access Management (IAM)

The vast majority of organizations (93%) believe integrating SOA/Web services security solutions with IAM is critical *(Figure 6).*

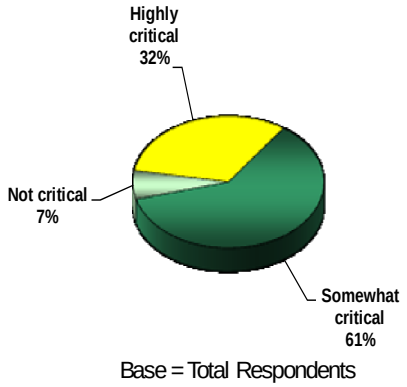


Figure 6: Criticality of integrating SOA/Web services security solutions with an organization's identity and access management solution.

93% of IT executives believe integrating SOA/Web services security solutions with IAM is critical.

However, just 43% have integrated SOA/Web services security solutions with the organization's IAM solution *(Figure 7).*

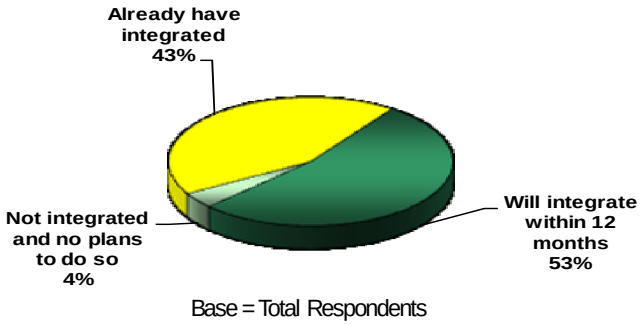


Figure 7: Status of integrating IAM solutions with SOA/Web services security solutions.

Despite the perception of criticality, just 43% of IT executives have integrated SOA/Web services security solutions with their IAM solution.

GMG Insights • 95 Nason Hill Road • Sherborn, MA 01770 P: 508-545-1095 | F: 866-725-7059

www.gmginsights.com

Organizations can be grouped by maturity and level of risk

This survey revealed that organizations fall roughly into one of four maturity categories based on the number of SOA or Web services security solutions they have implemented. At a macro level, each maturity category follows a similar pattern of maturation.

The pattern of maturation starts with the beginning of SOA/Web application development with little or no security measures in place. Service development activities are slowed as the organization recognizes the threat of exposure and begins to implement more security solutions to mitigate that risk. It is interesting to note the most mature organizations are more likely to have externally facing services and see the need for integration with IAM solutions.

Most companies recognize significant current exposure

Companies around the world, whether enterprise or mid market, are surprisingly similar in the pattern of their adoption of security solutions for SOA/Web services implementations. Generally companies have a direct correlation between the number of security solutions they have implemented and the status of SOA or Web services applications implemented – the more security solutions in place, the more SOA or Web services applications they will have implemented *(Figure 8).*

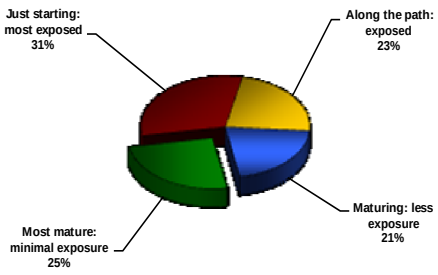


Figure 8: Adoption maturity of security solutions for SOA/Web services applications.

More than 50% of IT executives are exposed to security risks because of a lack of SOA/Web services security solutions.

GMG Insights • 95 Nason Hill Road • Sherborn, MA 01770 P: 508-545-1095 | F: 866-725-7059

www.gmginsights.com

The majority of organizations have a long way to go

Only about 25% of the market can be considered advanced in their deployment of security for SOA and Web services applications *(Figure 9).*

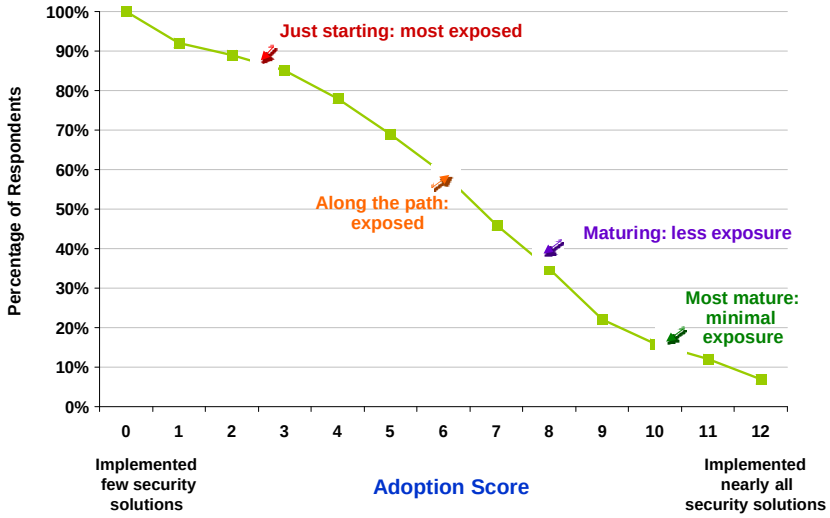


Figure 9: Spectrum of security solutions adopted for SOA/Web services

Just a small percentage of organizations have significantly reduced their exposure to the risks of SOA/Web services implementations.

Security is a constant and ongoing concern

Despite the number of security solutions the most mature organizations have in place, 44% still perceive security threats as a critical issue *(Figure 10).* It seems organizations have not yet reached a comfort level that the security solutions in place adequately protect them against the risks arising from SOA/Web services implementations.

Despite additional investments in SOA/Web services security solutions, even the most mature organizations still perceive the related security issues to be a critical threat.

GMG Insights • 95 Nason Hill Road • Sherborn, MA 01770 P: 508-545-1095 | F: 866-725-7059

www.gmginsights.com

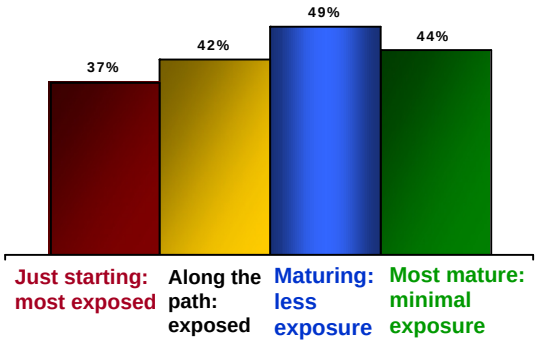


Figure 10: Percent each category ranking security threats as one of the "most critical" issues.

Adoption of standards is varied, signaling potential market confusion

Although SOAP[iii] is an integral part of many security standards, the percent of IT executives claiming to have adopted SOAP versus the other standards tested suggests there is a real lack of knowledge about standards today. The higher adoption of SOAP (and SOAP dependent standards such as Web services-security) versus REST[iv] would seem to indicate that there is a preference for more structured security and a concern for scalability of service-based collaboration.

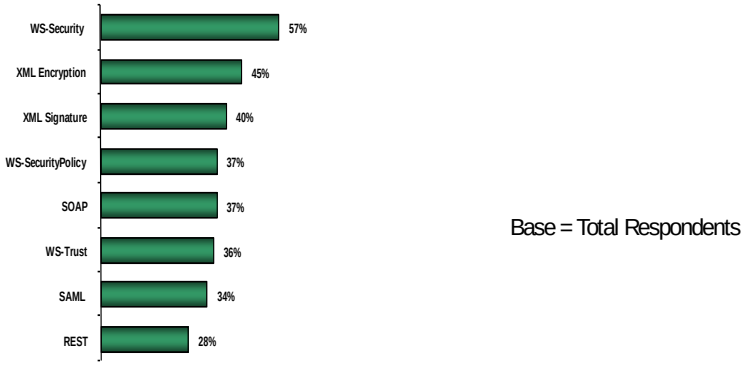


Figure 11: Security standards adopted, or to be adopted in the next 12 months, by organizations for SOA or Web services implementations.

SOA/Web services security standards are a mixed bag with no clear leader.

GMG Insights • 95 Nason Hill Road • Sherborn, MA 01770 P: 508-545-1095 | F: 866-725-7059

www.gmginsights.com

IT operations and IT security are in charge

While the VP of Application Development or head of enterprise architecture may be leading the charge to migrate to SOA and Web services based architectures, we see that the owners of enterprise security now govern the safety of service deployment. In the past that responsibility often resided with the developers themselves, but in what appears to be a sign of overall industry maturation the responsibility has centralized in the hands of the established security organization.

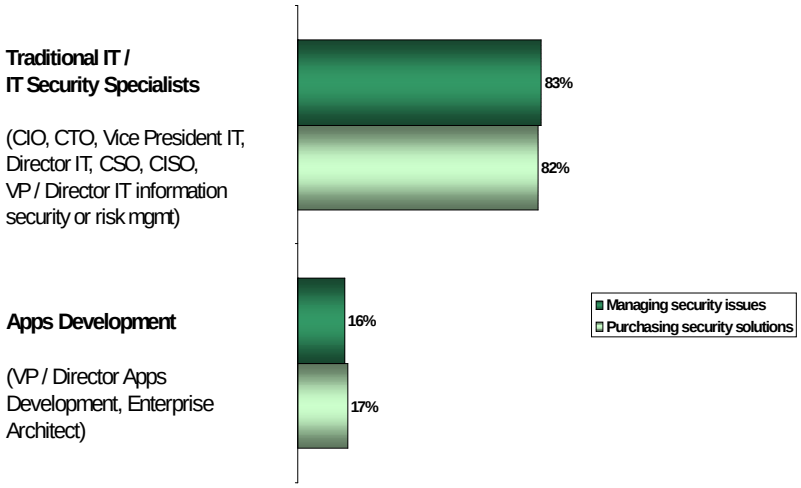


Figure 12: IT security is primarily responsible for security issues and solutions related to SOA/Web services implementations.

The IT security organizations have primary responsibility for SOA/Web services related security solutions.

GMG Insights • 95 Nason Hill Road • Sherborn, MA 01770 P: 508-545-1095 | F: 866-725-7059

www.gmginsights.com

The path to adoption of SOA/Web services security standards
The advantages of SOA and Web services application development will ultimately drive market maturation and further adoption of security standards and measures.

In many instances we have seen compliance with regulations drive the adoption of security strategies. In this study we found that the number of regulations an organization is subject to has little impact on its implementation of SOA or Web services security solutions.

The market is in its infancy. IT professionals know there are risks and, as a result, are proceeding slowly across the board. The pattern appears to be a quick jump into SOA development, likely driven by application development teams who see the broad benefits. Then when IT operations and IT security start to examine the associated risks, the organization slows down its SOA development to address security issues before moving aggressively forward.

This survey demonstrates that organizational comprehension of the risk increases as more security measures are taken and that even in the most mature organizations, the sense of vulnerability remains.

In the end, organizations will recognize the need to architect security measures from an enterprise perspective, taking into account the unpredictable nature of SOA and Web services applications and all the vulnerabilities they can generate. In many ways organizations are simply reliving the process many went through some 10 years ago with the deployment of today's websites and portals.

GMG Insights • 95 Nason Hill Road • Sherborn, MA 01770 P: 508-545-1095 | F: 866-725-7059

www.gmginsights.com

[i] For the purposes of this study, we defined **Service Oriented Architecture (SOA)** as a computer system's architectural style for creating and using business processes, packaged as services, throughout their lifecycle. SOA also defines and provisions the IT infrastructure to allow different applications to exchange data and participate in business processes. SOA separates functions into distinct units (services), which can be distributed over a network and can be combined and reused to create business applications.

[ii] For the purposes of this study, we defined **Web services** as software systems designed to support computer-to-computer communication across a network (Internet or intranet) using XML messages. Unlike traditional client/server models, such as a Web server/Web page system, Web services do not provide the user with a GUI. Web services instead share business logic, data and processes through a programmatic interface across the network and enable the respective organizations to integrate their applications without intimate knowledge of each other's IT systems.

[iii] **SOAP** is a protocol for exchanging XML-based messages over computer networks, normally using HTTP/HTTPS. SOAP forms the foundation layer of the Web services protocol stack providing a basic messaging framework upon which abstract layers can be built *(See Wikipedia).*

[iv] **Representational state transfer** (**REST**) is a style of software architecture for distributed hypermedia systems such as the World Wide Web. REST strictly refers to a collection of network architecture principles which outline how resources are defined and addressed. The term is often used in a looser sense to describe any simple interface which transmits domain-specific data over HTTP without an additional messaging layer such as SOAP or session tracking via HTTP cookies. These two meanings can conflict as well as overlap. It is possible to design any large software system in accordance with Fielding's REST architectural style without using HTTP and without interacting with the World Wide Web. It is also possible to design simple XML+HTTP interfaces which do not conform to REST principles, and instead follow a model of remote procedure call. The difference between the uses of the term

"REST" therefore causes some confusion in technical discussions *(See Wikipedia).*

GMG Insights • 95 Nason Hill Road • Sherborn, MA 01770 P: 508-545-1095 | F: 866-725-7059

www.gmginsights.com