

# CA Advisor

SECURITY MANAGEMENT NEWSLETTER

January 2009

## Security: Looking Back on 2008 and Ahead to 2009

By Bill Mann and Dave Hansen



The security outlook for this year is greatly influenced by the economic events of late last year. Looking back on 2008, it is now clear that October was the month companies started to understand that the financial downturn was very serious. It wasn't until early December that

the National Bureau of Economic Research called an official recession — one that had truly started a year prior in December of 2007.

As our government takes strides to jump-start the economy and save and create jobs, we anticipate seeing the area of security compliance broaden. We also anticipate organizations will continue to invest in security, but with an increased level of pragmatism as they tightly scrutinize budgets and return on investment. Companies more than ever will be looking for ways to improve operations while reducing costs.

Even before October 2008, organizations were investing in technologies such as virtualization and Software-as-a-Service (SaaS), such as Salesforce.com, to help reduce costs. Implementing virtualization technologies and using SaaS for outsourced applications may save money, but they also present new security challenges.


It is clear that virtualization can bring many benefits to an organization, but it also increases the risk profile of the host servers and raises a new set of security and access concerns. For example, there are an increasing number of compliance regulations and privacy directives companies

must follow. As companies employ virtual servers in greater volume to run production applications and store sensitive data, they are exposing themselves to a higher level of risk on the host server and some important new risks on each of the virtual or "guest" machines.

The challenge is obvious. As more resources and applications are placed and run on virtual servers, businesses need to protect that data in the same way they would protect data on their physical servers. There are several areas of concern that are not addressed in many virtualization deployments because they are not currently covered by virtualization software or native operating systems:

- Critical file protection, monitoring and other operating system hardening measures;
- Role-based access rights for administrators and segregation of duties;
- Detailed auditing;
- The ability to adjust security levels and policies regularly to match the flexibility of the virtual environment.

SaaS applications can be financially compelling for organizations. They allow companies to focus on business initiatives while a third party develops, hosts and operates the application and the infrastructure supporting it. However, like any other application, SaaS applications need to be secured. They can become an added risk factor in any risk analysis as they are hosted outside an organization. Access control technologies with the ability to authenticate a user based on identity and policies are needed to secure access to the remotely hosted application.



As we move into 2009 and the effects of the recession become more tangible, security compliance will continue to drive security initiatives. This will drive the need for Identity and Access Management (IAM) solutions. Tightened regulations across industries as well as new mandates surfacing to govern financial institutions that have received government assistance will drive security compliance efforts.

IAM solutions include technology to provide identity lifecycle management. This year, access management's automated role-management capabilities will be essential as companies make reorganize or reduce staff. They'll need to quickly provision new employees and make sure that existing employees who are taking on more responsibilities get the right access in a timely fashion.

Among organizations that have implemented role-based IAM, we are likely to see introduction of more sophisticated features to achieve smart provisioning through role-based management. Such efforts could pay off as internal auditors pressure the security department for proof that retired accounts have indeed been deactivated, for example.

Finally, data loss and leakage will be a hot topic over next year. As the economy drives a work environment with turnover and reorganization, it also creates an atmosphere for misuse of data and even data theft. Most companies have no ability to track this data misuse or loss. This will drive a combination of data loss prevention (DLP) technologies with identity and access management technologies for a more comprehensive information security solution. With DLP and IAM technologies combined, customers can now control who has access to what information and what they can do with that data once they access it. It also will offer an auditable trail, further helping to ensure compliance.

We expect 2009 will have an increased interest in security, as the global economic environment is likely to create more complexity internally as well as externally. On the inside, identity and access management will be in unprecedented demand for increased security and improved operations while helping ensure compliance. And outside the organization, certain sectors like financial services will require new government regulatory measures for security and compliance.

---

*Dave Hansen is Corporate Senior Vice President and General Manager of the Security Management Business Unit at CA. As general manager Dave is responsible for developing CA's security management business and ensuring the team is delivering the products, services and partnerships required to meet customer needs for strategic, enterprise level security. Previously, Dave was CA's Chief Information Officer, responsible for global IT strategy, applications development and the global CA infrastructure, IT compliance and CA's international IT organization. Dave joined CA in 2002 and has more than 20 years of professional experience leading IT organizations. Prior to joining CA, Dave led IT for the Canadian division of Bowater Inc., where he was responsible for IT infrastructure, technology acquisition/integration and ERP implementation.*

*Bilhar (Bill) Mann is a Senior Vice President in the Security Management Business Unit at CA. He is responsible for product strategy, product management and business development. Bill has had numerous senior positions within CA's security business unit covering technologies including identity and access management, security event management and threat management.*

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