



*High performance. Delivered.*

## Managing the Risk of Technology Innovation

Security approaches that keep pace  
with innovation and contribute to  
high performance

By Paul O'Rourke, Alastair MacWillson and Bjørn Arne Berge

• Consulting • Technology • Outsourcing

Amid economic uncertainty, there is an acute need for businesses and governments to mitigate threats to profitability and revenue and ensure cost structures are as lean as possible. Today, addressing enterprise risk means balancing interrelated organizational priorities, such as technology innovation and information technology (IT) cost reduction, in the context of an overall risk management strategy.

Pressure to save money means IT cost structures must evolve because technology spending is often a ripe target for reduction measures. Fortunately, technology innovation can assist with reducing costs, but the challenge for chief information officers (CIOs) is that such innovation typically also fosters risk and complexity. For this reason, innovative projects must be undertaken hand in hand with security initiatives.

## Key Enterprise Trends

For the foreseeable future, enterprise security must embrace three key trends:

### Cloud computing and SaaS

Sourcing IT solutions from multiple content and service providers—using either a cloud computing or software-as-a-service (SaaS) approach—unlocks data held in IT silos. This increases risk by enabling confidential enterprise data to cross unsafe boundaries, and the cloud itself presents risks since organizations have less control over infrastructure.

Since their core business is based on securing customer data, major cloud providers have made progress in this area. In fact, many of them offer more sophisticated end-to-end, base-level security and privacy protection than might be found in the data centers of any single enterprise. However, there are still many open issues such as data control and certification. The pace of uptake will depend heavily on how soon these issues are resolved and when cloud providers will be able to obtain official certification of their security practices from independent third parties.

### Lightweight systems integration

Taking advantage of Web 2.0-based collaboration tools, including 'mash-ups' that combine disparate data stores in easy-to-use interfaces, can be an innovative way to improve productivity. Unfortunately, such user participation can lead to an increase in employees sharing sensitive enterprise data—anytime, anywhere, via any device.

### CIO as data custodian

Conflict of interest among consumers, governments and companies leads to an ever-increasing and constantly shifting group of data-protection laws and regulations at a local, state and national level. It is a challenge to interpret and adhere to regulations that address areas as diverse as mergers and acquisitions (California Act SB 1389), non-public information disclosure (Gramm-Leach-Bliley Act), financial reporting (Sarbanes-Oxley Act) and data privacy (European Union Data Privacy Directive). In response, CIOs must address diverse commercial priorities via myriad compliance, governance and risk measures; enterprise policy management; and secure business-process management.

## How Effective Are Current Data Security Practices?


It is an opportune time for CIOs to proactively and strategically advise on safeguarding data assets and adopting new technology while encouraging their organizations to meet compliance, IT cost reduction and risk-management goals.

A crucial task for CIOs is to institute airtight approaches to security. This is particularly important so that organizations can quantify risk in step with cost-reduction imperatives and corresponding technology innovations.

A case in point is regulation and compliance. CIOs should counsel their organizations to avail themselves of policies and practices that enable compliance with draft legislation on privacy breaches, and that allow close monitoring of threats to the enterprise landscape.

Accenture recommends CIOs examine the effectiveness of their security strategy in addressing:

**Data as a strategic asset**—Organizations collect vast amounts of data to support business processes, and employee, customer, partner and supplier



interactions. A security software firm has estimated the average value of information held on a typical corporate laptop at nearly US\$1 million. The goal is to leverage technology to protect privacy but still allow for legitimate data use and selective disclosure.

**Consumable security**—Organizations use common security approaches that define processes, procedures and mature technology stacks. Consumable security, in contrast to emerging strategy security assets, includes security for the perimeter of the enterprise or extended enterprise, from intrusion detection systems to intrusion protection systems.

**Secure business processes**—As service-oriented architecture (SOA) is growing in influence and prominence, organizations need to assess not only their own IT security but also that of the extended enterprise so that legislative compliance and risk are not compromised.

## What to Do Now? Five Ways to Improve Security and Mitigate Risk

Accenture has five recommendations for organizations seeking to manage data as a strategic asset, harness consumable security and build secure business processes.

### 1. Ensuring cloud security

The most important concerns inhibiting organizations from progressing with their enterprise cloud strategies relate to the security of data transmission, the physical security of cloud vendor assets and the transmission of data via the Internet beyond the enterprise firewall. Data transmission security can be overcome with encryption. Physical security issues can be assessed with independent audit and certifications. Finally, exposure to the Internet can be addressed by careful management of user identities and firewalls such as Amazon's Elastic Compute Cloud (EC2).

As a result, enterprises that are progressing with enterprise cloud strategies and deployments need to focus on service providers who:

- Can offer them secure connectivity
- Are willing to undergo independent audit and certifications of their security practices in the extra-enterprise cloud
- Can be fully compliant with the organization's compliance, auditing and security policies
- Can comply with the official standards for cloud computing (though these standards are still evolving)

### 2. Design security for mass collaboration

Organizations will need to increasingly push decision making and process control out to the edges of the organization, delivering information with the appropriate level of protection to the broadest possible base of constituents.

### 3. Anticipate IT asset diversity

As the number of applications and users surge, so too does the complexity of managing associated identity and access management rules. For each additional application to which users gain access, organizations must provide fine-grained entitlement, including a user interface, data and business logic. That is why organizations need to provide a unique identifier for services accessed by internal and external users. They must also take steps to reduce the cost and complexity of demands driven by partners and outsourcing. In addition, because composite solutions and reusable utility services stretch across multiple systems, organizations need to better manage security decisions, provisioning steps and administrative tasks.

#### 4. Incorporate alternate digital-identity styles

Organizations should determine how to maintain order in a society where people are increasingly online; identity information cannot be centralized for privacy reasons; and resources that do not belong to a single domain and common identifiers, such as country of birth and social security numbers, are overused. Incorporating alternate styles of digital identity includes allowing users to have more control of their digital identity, while enabling security claims to cross domains by being portable and interoperable. For organizations, this means also ensuring that users continue to have a digital identity for clearly bounded domains—for example, expense management, finance and human resources applications—that are administered centrally.

#### 5. Implement secure business processes

Accenture anticipates that clients will soon use SOA in the vast majority of mission-critical operational applications and business processes. Organizations must address this shift in the IT

landscape with SOA security principles that mitigate 'process-centric' security risks, enable a unified view of customers or entities, model security within workflows and business orchestrations, transfer security claims across untrusted boundaries and assure the integrity of multi-party transactions.

### Helping You Achieve High Performance Through Improved Data Security

Accenture helps businesses and governments achieve high performance by addressing enterprise risk and resulting security challenges. We harness our deep experience to assist clients with reducing IT expenditure using a targeted approach that identifies cost-reduction targets in the context of maintaining compliance, risk and security.

Accenture collaborates with clients using a proven approach that includes investigating an organization's risk profile, regulatory compliance challenges and IT governance issues, then segmenting areas suitable for intervention, such as discrete business divisions. As appropriate, Accenture

evaluates potential security solution providers from a technology-agnostic perspective to determine which ones offer the right level of maturity for each client.

As part of Accenture's suite of proven tools and methodologies, we identify and analyze technology investment plans, determine the impact of new technology on business processes and closely assess whether proposed cuts to IT cost inadvertently compromise security and increase an organization's risk.

To further assist organizations on the journey towards high performance, Accenture's capabilities enable our experienced professionals to team with clients on diverse engagements. These include data protection and privacy, data protection and security around SAP and Oracle technologies, enterprise threat landscapes, core enterprise protection at the perimeter of the organization and/or extended enterprise, and security approaches for preventing sophisticated penetration of core financial applications.

Copyright © 2009 Accenture  
All rights reserved.

Accenture, its logo, and  
High Performance Delivered  
are trademarks of Accenture.

For more information,  
please contact:

**Paul O'Rourke**  
[p.orourke@accenture.com](mailto:p.orourke@accenture.com)

or

**Bjørn Arne Berge**  
[bjorn.arne.berge@accenture.com](mailto:bjorn.arne.berge@accenture.com)

#### About Accenture

Accenture is a global management consulting, technology services and outsourcing company. Combining unparalleled experience, comprehensive capabilities across all industries and business functions, and extensive research on the world's most successful companies, Accenture collaborates with clients to help them become high-performance businesses and governments. With more than 181,000 people serving clients in over 120 countries, the company generated net revenues of US\$23.39 billion for the fiscal year ended Aug. 31, 2008. Its home page is [www.accenture.com](http://www.accenture.com).