WHITEPAPER

salesforce.com
Success On Demand.™

Busting Myths of On-Demand: Security (July 2007)

Peter Coffee
Director, Platform Research
pcoffee@salesforce.com

Contents

Myth:
On-demand convenience and economy bear a price tag of security risk

When a CIO first considers on-demand options, they may seem to entail high risks as vital databases migrate to external systems. That concern, though not without merit, is readily controlled when working with an enterprise-class service provider. Far more of an overlooked, everyday risk is the overworked, often under-trained in-house operator, or the fully authorized end user more concerned with simplicity than security.

On-demand systems, designed from the bottom up for multi-tenant privacy and under constant expert supervision and scrutiny, offer a compelling security edge over most on-premise IT installations.

Busted:
On-demand systems, rigorously designed and administered, reduce the real-life risks of misconfiguration, loose procedures, and error or abuse by in-house staff.

Security at salesforce.com

Protecting enterprise data and business processes requires multidisciplinary expertise and relentless attention to detail. Customers of salesforce.com can see its superior physical security, beginning with anonymous data-center exteriors and secure on-site storage of backup media. Customers can see the precision and convenience of salesforce.com features for defining security rules, assigning user profiles, and auditing field-level histories of who changed what information at what time.

Less visible are the formal security certifications for salesforce.com personnel and systems, the secure network architecture, and the superset effect in which the security standards of the world's largest financial institutions drive the entire salesforce.com platform—protecting customers of every size.

Security has been a salesforce.com priority from day one—and it shows

Read on for more

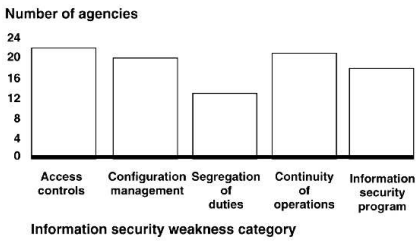
Enemies within: carelessness and malice inside the firewall

In-depth examinations of information security risk rarely result in full public disclosure of findings, since attackers are likely to exploit such knowledge far more quickly than organizations can respond with remedial measures. A useful exception is United States Government Accountability Office GAO-07-935T, a report released on June 7, 2007 and presented in testimony to Congress by Gregory C. Wilshusen, Director for Information Security Issues in that agency.

As summarized by the figure below, reproduced from that GAO submittal, a study of 24 "major federal agencies" found that "significant weaknesses in information security controls threaten the confidentiality, integrity, and availability of critical information and information systems used to support…operations, assets, and personnel…" Specifically, the GAO reported to Congress that

> Almost all of the major federal agencies had weaknesses in one or more areas of information security controls (see figure). Most agencies did not implement controls to sufficiently prevent, limit, or detect access to computer networks, systems, or information. For example, agencies did not consistently identify and authenticate users to prevent unauthorized access, apply encryption to protect sensitive data on networks and portable devices, and restrict physical access to information assets. In addition, agencies did not always manage the configuration of network devices to prevent unauthorized access and ensure system integrity, such as patching key servers and workstations in a timely manner; assign incompatible duties to different individuals or groups so that one individual does not control all aspects of a process or transaction; and maintain or test continuity of operations plans for key information systems. An underlying cause for these weaknesses is that agencies have not fully or effectively implemented agencywide information security programs.

Information Security Weaknesses at Major Federal Agencies for Fiscal Year 2006



Source: GAO analysis.

On-premise is not the ideal

- :: Authentication measures are not consistently applied
- :: Encryption is often poorly administered or unused
- :: Patch application, testing of continuity procedures may be informal and/or infrequent
- :: Physical access to IT assets, separation of IT duties often fail to reflect best practices
- :: Central administration of on-demand systems offsets the net exposure of data in secure external storage

Largely as a result of such lapses from best practice in organizations generally, it's estimated[1] that $^4/_5$ of IT-related attacks arise within the organization—according to security professional Michael Bruck, founding partner of Chicago-based BAI Security. Others agree: "Most incidents have their root cause in intentional or non-intentional lack of compliance on the part of employees," according to Kavitha Venkita, practice manager of the Information Risk Executive Council in Washington, D.C.[2]

Bruck's estimate is not inconsistent with study results reported[3] in May 2007 by Newton, Massachusetts-based Cyber-Ark Software, whose survey of more than 200 IT professionals found $^1/_3$ of them actually admitting to abuse of their administrative access privileges to examine sensitive data unrelated to their job functions. About $^1/_4$ reported knowledge of former employees who retained access to "sensitive networks" long after their termination, with $^1/_3$ stating a belief that they could do likewise with little risk of detection.

Employers are understandably reluctant to impute actual malice to their own employees, but the roles of simple carelessness and ignorance are also significant. A survey[4] of 477 attendees at an information security conference, presumably not the worst-case population for careless data handling, found them estimating that they had each lost an average of two to three data storage devices such as USB memory keys. There's little reason to hope that any sizable fraction of those devices used encryption to protect their contents.

It is therefore clear that an in-house code base and on-site data storage can not be realistically treated as an ideal reference case, with outside providers necessarily increasing risk. The formal procedures, certified training, and frequent independent assessments undergone by an enterprise-class service provider should rather be considered the standard that most in-house operations can only aspire to match.

[1] Bruck, Michael, "Security Threats From Within," entrepreneur.com, 28 June 2007
[2] Kaplan, Dan, "Educating the masses for IT security," SC Magazine, 14 June 2007
[3] "Survey Reveals Scandal of Snooping IT Staff," Cyber-Ark Software Inc. press release, 30 May 2007
[4] Utimaco Safeware AG press release, 23 January 2007

Good things to excess: origins of new risk in a networked world

In addition to internal organizational risks, it's crucial to recognize the technical risks of client-server models that rely on complex client applications combined with local data storage and other client-resident state.

Convenient to a fault

With the 1994 emergence of Web browsers, and the 1996 debut of 56 kbit/second modems, computer communication morphed from point-to-point conversations between trusted partners into an orgy of any-to-any interaction. This turned out to have the same drawbacks in the digital domain that it does in other realms.

When a PC user had to dial up a low-speed connection to an on-line service, that act gave informed consent to limited forms of data exchange. Text-based "bulletin boards," accessed through terminal emulators or dedicated applications, had no means of altering the functions of client machines. The domains of content and behavior—of data and code—were distinct.

That useful boundary was fatally compromised by Microsoft's 1996 introduction of ActiveX Controls: a specification for software components with intrinsically insecure design. Though not unique in this regard, ActiveX was archetypal in its emphasis on developer capability and end-user convenience rather than secure and controllable behavior—and even a decade later, ActiveX continues to be a powerful tool for attackers.[5]

- Designed to be self-registering, ActiveX controls eliminated the need for user consent to the introduction of new code onto a client machine.
- Designed to be composable into graphically interactive applications, ActiveX controls eliminated visual cues to the presence of code from multiple and perhaps untrusted sources in what appeared to be a monolithic application.
- Designed for single-user, stand-alone machines, ActiveX controls proceeded from an assumption that a component should enjoy all the operating privileges of its user: "an extremely insecure way to provide a feature," in the words of Microsoft's own documentation[6], since "from the moment a user downloads an ActiveX control, the control may be vulnerable to attack because any Web application on the Internet can…use the control for its own ends…"

Local users left out of the loop

:: Always-on connections, high-bandwidth links facilitate malicious background tasks

:: Desire to minimize apparent complexity makes it too easy for "smart content" to alter system behavior and state

:: Origin of PCs as isolated systems creates legacy assumption of administrative powers in too many non-system applications and tools

:: Improvement depends on granular privilege management and minimal leakage of data to network edge

Web pages thus acquired various means of presenting executable content, and injecting that content persistently into a PC user's environment. This process was accelerated by early "wars" among browsers whose feature-driven evolution was slow to make security a priority—and the enterprise role of "PCs plus Internet" access has been threatened thereby. By June 2007, for example, the FBI estimated[7] that more than one million personal computers had become enlisted in so-called "botnets" of centrally managed network nodes, running many different forms of malicious software without their owners' knowledge.

- Without the any-to-any connectivity of the wide-open Web, users would unlikely to encounter the malicious parties who use both technical means and social engineering to attract their targets.
- Without the concurrent dramatic growth of end users' Internet bandwidth, surreptitious download of malicious code or unauthorized upload of data could not take place unnoticed by PC users.
- Without the generous processing power of current PCs and their multi-tasking operating systems, marketed for such CPU-intensive tasks as home video editing and interactive gaming, malware's burden on machine resources would be far more apparent and more likely to be detected.

Resolving to do better

The PC and the Internet have thus twisted their own extraordinary improvement into the degradation—though not the complete destruction, at least not yet—of their own utility. Prudent enterprise IT architects recognize the likely prospect, going forward, of more of the same—and are therefore seeking more transparent and governable models for handling critical data and executing line-of-business functions.

The next generation of secure IT depends on connection to known facilities running a known base of code, with minimal transfer of data from the secure center to the uncontrolled edge of the network. Rather than relying on individual users to exercise administrator-level discretion, the applications exposed to end users must be designed to define and manage users' access in a granular manner—a "need to know" model—and must steer clear of the swamp of dubious code that constitutes the modern PC operating environment.

On-demand applications, accessed through industry-standard Web browsers and eschewing specialized client modules that represent sources of vulnerability and points of attack, offer a promising option.

---

[5] Gaudin, Sharon, "iPhone Used as Bait for Malicious Web Site," *InformationWeek*, 2 July 2007
[6] "Designing Secure ActiveX Controls," Microsoft Knowledge Base document Aa752035
[7] Cooney, Michael, "FBI Finds Over 1 Million Botnet Victims," *NetworkWorld*, 13 June 2007

Rising expectations: rejection of "business as usual"

Rising awareness of IT threats has taken the subject of information security far beyond the domain of discussion by only technical or law enforcement professionals. The office of the attorney general for Ohio estimates[8] that identity theft cases in that state are growing by 20 to 30 per cent per year; a Canadian survey[9] has found $^{2}/_{3}$ of citizens aware and concerned about the issue, with $^{4}/_{10}$ believing that they are personally likely to become victims at some time to come.

Data breaches ranging from individual celebrities' cellular phone records[10] to hundreds of thousands of employees' personal information[11] or even 1.3 million voters' identification data[12] have made IT security a topic of mainstream news stories and a subject of community seminars.

Massive incidents such as the TJX data breach, estimated[13] as of May 2007 to have cost more than $17 million to date in remediation expenses and legal fees, rebut the notion that in-house systems represent the prudent choice from the security point of view. Customers now know better.

It is therefore time to leave behind the notion that IT security should not be mentioned at all, for fear of scaring the customer. In the same way that it was once said[14] that "safety doesn't sell" in the automobile industry, a proposition now clearly refuted[15], it is time for all customer-facing organizations to have a strong story to tell about their high regard and unimpeachable practices for keeping customer information safe.

With industry-leading protection of the application, the network, and the physical facility, salesforce.com's on-demand platform gives its customers confidence that their security story will meet every expectation.

For more information about security for salesforce.com products, download the salesforce.com white paper,[16] "The Seven Standards of Service Delivery."

[8] Strickland, Waylon, "Assistance, awareness for victims of ID theft," Circleville *Herald*, 8 June 2007
[9] Sigma Assistel press release, 13 June 2007
[10] "X-rated Paris Hilton site exposes customer information," networkworld.com, 15 June 2007
[11] Fisher, Dennis, "Data breach at Boeing exposes 382,000 employees," SearchSecurity.com, 13 December 2006
[12] "Discs exposed Chicago voters' personal data," Associated Press, 22 January 2007
[13] Gaudin, Sharon, "Breach costs soar at TJX," *InformationWeek*, 21 May 2007
[14] Dowie, Mark, "Pinto Madness," *Mother Jones*, September/October 1977
[15] Lovel, Jim, "CP+B, VW Try the Shock Treatment," *AdWeek*, 24 April 2006
[16] www.salesforce.com/assets/pdf/datasheets/SevenStandards.pdf

For More Information

Contact your account executive to learn how we can help you accelerate your CRM success.

The Americas
The Landmark @ One Market
Suite 300
San Francisco, CA 94105
United States of America
1-800-NO-SOFTWARE
www.salesforce.com

Latin America
Alfonso Napoles Gandara 50
4th floor
Col. Santa Fe
Mexico City
Mexico 01012
+52-55-9171-1882
www.salesforce.com

Japan
Ebisu Business Tower 18F
1-19-19 Ebisu, Shibuya-ku
Tokyo, 150-0013
Japan
+81-3-5793-8301
www.salesforce.com/jp

Asia/Pacific
9 Temasek Boulevard
#40-01 Suntec Tower 2
Singapore 038989
+65-6302-5700
www.salesforce.com/au

Europe, Middle East & Africa
Ch. de la Dent d'Oche 1B
1024 Ecublens
Switzerland
+353-1-2723-500
www.salesforce.com

salesforce.com® Success On Demand.™