Friday, June 15, 2007
Vol. 23, No. 11

Soft•letter

BUSINESS INSIGHTS FOR SOFTWARE DEVELOPERS & PUBLISHERS

Mark the Date!

Softletter's Marketing and Selling SaaS Seminar
Santa Clara, CA
October 3/4

The key to VC is SaaS: for Q1 2007, 40 of the top 50 deals involve companies with recurring revenue models
See pages 4-5.

Providing Your Customer With a SaaS Security Blanket

One of the primary reasons for the collapse of what was then called the ASP market in the period from 1999 through 2001 was the skepticism of enterprise customer's over the ability of SaaS companies to provide adequate security for customer data. "We'll never let that type of data out of our physical control" was the retort of many, many members of upper management. And at the time, few software companies were well prepared to deal with security objections.

But things are changing rapidly in the software industry, as you can see from our analysis of where today's VCs are placing their monetary bets. To help software companies understand how to discuss SaaS security with enterprise customers, we sat down with John Shovic, VP of Business Development for InstiComm, a developer of mobile communications services for doctors. InstiComm's products transmit patient's medical and billing information wirelessly and if there's one business where privacy concerns are vital to your business model, it's in the healthcare industry. As the former CEO of TriGeo Network Security, professor of Cyber-Security at Eastern Washington University, and CTO of MiloCreek, a consulting and services firm specializing in cyber-security, John is uniquely qualified to discuss this topic.

John, how should SaaS companies address questions and skepticism about the ability of their firms to manage customer's data securely and safely?

One important component is education and realizing who needs to be educated in the corporate hierarchy. Often, the main objections will be coming from upper management, not IT. One approach I've found consistently effective is to point out to executives how many systems that support their business and on which they rely, both directly and indirectly, are built on the SaaS model, even if they (the executive), doesn't realize it.

For example, small and regional banks are increasingly not attempting to build their own IT infrastructures but turning to companies such as Fiserv to provide their core capabilities. (And even the larger banks, while they manage their own IT systems, provide services to their branches via a SaaS model.) In medicine, smaller and

(continued on page three)

Publisher & Managing Editor
Merrill R. Chapman
rickchapman@softletter.com
860/663-0552

Editor
Donald K. Rosenberg
don@softletter.com
919/687-4172

Editor Emeritus
Jeffrey Tarter
jtarter@softletter.com
617/668-0028

Editorial office
Soft•letter
34 Sugar Hill Rd.
Killingworth, Conn.
06419
Voice: 860/663-0552

Subscription office
Aegis Resources
34 Sugar Hill Rd.
Killingworth, Conn.
06419
Voice:860/663-0552
Fax: 860/663-0553
info@softletter.com

www.softletter.com

Software Licensing and the GPL, Part I of II

Jeff Gordon, The Software Licensing Handbook

Software licensing used to be relatively straight forward. The software vendor set a price and a licensing metric. The buyer decided if they were willing to pay the price. If so, buyer and seller signed a license that described the relationship and the usage rights for that specific software. In almost all cases, use was limited—and if the buyer wanted to do something more than just use the software, they had to go back and ask the vendor for permission.

This basic structure held together for about 30 years. As software became more complex, so did the licenses supporting that software. MIPS-based licenses transitioned to various forms of user-based licenses. Coming full circle in the last few years with the proliferation of SaaS relationships, the industry is now back to usage-based licensing (similar to MIPS in many ways). Again, however, anything beyond basic use of the product still requires additional permission—especially if it involves the incorporation of software from one vendor into the software product of another vendor.

There¹s a new player in town, however, and his name is "free software." No, not free as in "without cost," but free as in the freedom to use the software in a less restrictive manner. This first distinction is not trivial; in fact, it is how a company like RedHat can be profitable. Free software can be sold. What we're concerned with here is the usage. Generally speaking, free software licenses state that when the object code is distributed, so must the source code, and that once licensed, the buyer is free to give away copies of what they bought in an unrestricted manner (adhering only to the license document).

The GNU General Public License (GPL) is the flagship software license for use with free software. Currently on version 2 (with version 3 almost at the point of release), the GPL is widely regarded as the founding father of free software (Use of the term "open source" is sometime used synonymously with "free software." The Free Software Foundation, however, prefers the term "free software" when used in discussing the GPL). The GPL is the path to a concept known as "Copyleft." Whereas, in the Free Software Foundation's view, copyright is used to restrict usage, copyleft is used to confer unrestricted usage. These terminology issues can be confusing, but are quite important for the ideological viewpoints that are the driving force behind the use and proliferation of free software. If a software developer chooses to release their software in a copyleft manner, they will use the GPL as a way to ensure that the code can not be further restricted. Using the GPL, however, adds restrictions which will deter a future user of the code from integrating it into, or using it in conjunction with, their own proprietary product. Knowing these restrictions is absolutely essential to prevent a license violation.

As of the end of May, 2007, the GPL essentially stands alone with the copyleft concept. For this moment in time, then, a software developer can know that software released under the GPL taints non-GPL software if it is linked (statically or dynamically) with that non-GPL code. The taint requires that the once-proprietary code now be released under the terms of the GPL. From an ideological perspective, this is one of the goals of the Free Software Foundation and their Free Software Definition (see www.fsf.org).

Jeff Gordon, author, The Software Licensing Handbook, 9304 Cub Trail, Raleigh, N.C., 27615; 408/954-3977. E-mail: jgordon@avaya.com. Website: www.licensinghandbook.com.

regional hospitals are already moving to SaaS models for their record storage and transmission needs; nobody is coding their own systems anymore and hospitals are trying to shed IT costs as quickly as they can. Examples of this can be found all over the country; the Providence hospital chain in Seattle, for example.

Now, banking and healthcare are industries that have to deal with incredibly strict regulatory regimes. With my company, which operates on a SaaS model, every part of our infrastructure needs to be HIPPA compliant, from the software to the servers and phones. In banking, the FDIC can shut your business down and make you personally liable for loss and damages if you've not done your due diligence in terms of protecting customer privacy. The question you should be asking potential customers is: "If those industries believe they can rely on SaaS, why do you think your industry can't?"

"The SaaS model is also increasingly taking hold in the securities industry, another industry that faces heavy security and privacy regulations. Smaller and regional brokerages rely on firms such as Dundee. They don't refer to what they do as SaaS, but that's what it is."

—John Shovic
InstiComm

Aren't you still going to have to provide assurances about the physical security of the data?

Yes, particularly when dealing with larger companies. Now, there are several approaches you can take to assure customers that you are able to protect their data. But before we go through my checklist, the first thing you need to do is ask the customer how ready **they** are to protect their data. The reality is that while customers may have physical control of their data, they may not have in place the infrastructure to protect it from disaster, theft, and intrusion. A SaaS company should be ready to conduct a security audit on behalf of potential customers, and point out the customer's security weaknesses and problems. For example, is the server room located in a fire and heat proof facility? Do you hire armed guards to protect your building?

"Paradoxically, SaaS is becoming easier to sell in industries with heavy privacy and data security regulations. This is because you have a regulatory framework that you can study and then demonstrate you adhere to."

—John Shovic
InstiComm

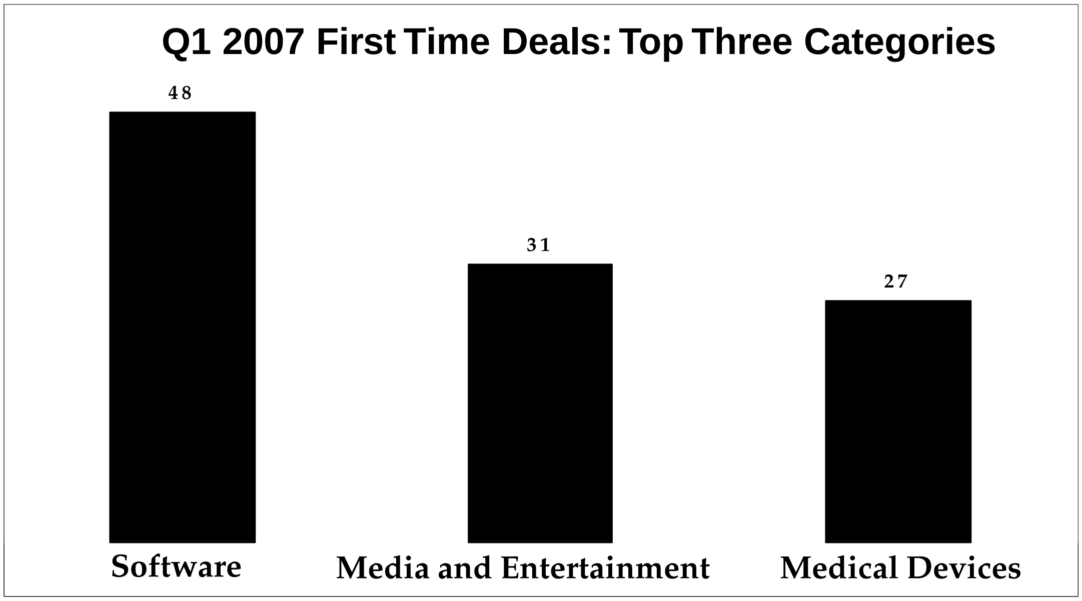
And you need to be armed with facts such as the reality that in 2004, a Yankee report found that 42% of companies reported they'd experienced a tape backup failure. Most tape backups are not encrypted, so if someone walks out with a tape, you can suffer an immediate and dangerous privacy breach. And that 60% of intrusions and security breaches are **internal**.

Now, let's turn to the issue of what a SaaS firm needs to demonstrate that its operations are secure. First, particularly when dealing with larger customers, you're going to need to provide proof that your company adheres to security standards: an audit.

Do you recommend a SAS 70 audit?

If you can afford it, but they're expensive. If you're going to undertake SAS 70, I'd plan on budgeting $100k+. But if your budget is not up to this, or you don't think your market requires SAS 70 certification, there are other, but still credible alternatives. For instance, the big three accounting firms all offer audit and certification programs (as well as

(continued on page six)



Benchmarks: Q1 2007 Venture Capital Investments

Though Q1 2007 did not yield as many first time venture capital deals as the previous quarter, software was the recipient of the most first time investments, receiving 48. However, this quarter saw also saw biotechnology supplant software's usual place at the top of the VC food chain with $1.5b in investments contrasted with $1.1b for software. Network related companies, which includes the security, wireless, networking, and telecommunications categories, all heavy consumers of software, received $2.5b during the first quarter. This was on a fairly even keel with the $2.4b that was invested in Q4 2006 but was down from the $2.8b invested in Q1 of 2006.

In previous issues of Soft•letter we've made note of the fact that the vast majority of new venture money flowing into US software forms is going to companies with a recurring revenue business model. An examination of this quarter's deals bears this observation out; of the top 50 companies listed, our analysis identified 40 of them as either SaaS or recurring revenue plays.

The trend of infusing larger amounts of money into fewer companies is also continuing; the number of companies receiving significant investment deals dropped from 266 in Q4 2006 to 223 in Q1 of this year. Biotechnology and medical devices amounted to 36% of Q1 2007 dollars, a record high for the industry. Medical and biotechnological companies require substantial funding in order to complete regulatory or statutory processes and VC's ponied up the needed dollars. However, an analysis of some of the largest bio-tech companies raises the question of whether some of them should be thought of as software companies as well? Many of the core technologies which these firms have developed use software systems of extreme complexity and sophistication. A look at the Media and Entertainment sector also reveals a strong and growing software presence.

The material in this report is drawn largely from the Money Tree Survey by PricewaterhouseCoopers, Thomson Venture Economics, and the National Venture Capital Association, and generally confirmed, modified, or supplemented by other sources.

The Top 50: Software Venture Capital Investments—Q1, 2007

Company	Business Focus	Lead Investor	Investment
Automated Trading Desk	Automated trading	Technology Crossover Ventures	$60,000,000
Dexterra	Business process software	Canaan Partners/New Enterprise	$36,556,000
Market Force Information	Store-level retail information	Boulder Ventures/Centennial Ventures	$31,893,200
n2N Commerce	Cross-channel on-demand eCommerce	General Catalyst Partners	$30,000,000
DriveCam	Video systems for commercial transportation	Insight Venture Partners/Integral Capital	$29,000,000
ChoiceStream	Online consumer services	General Catalyst Partners	$25,790,100
Achievo Corporation	IT outsourcing	Undisclosed Investor	$24,000,000
Gearworks	Mobile workforce management	American Capital Strategies	$21,400,100
Mavenir Systems	Network convergence solutions	Alloy Ventures/Austin Ventures	$20,500,000
Gemini Mobile Technologies	Wireless software infrastructure	Goldman, Sachs & Co.	$20,000,000
Altierre Corporation	Wireless business for r retail	ATA Ventures/Kinetic Ventures	$17,000,000
Mimosa Systems	Email archiving company	August Capital Management	$17,000,000
Centrify Corporation	Security software company	Accel Partners/INVESCO Private Capital	$15,000,100
Scansafe	Web security-as-a-service	Benchmark Capital/Scale Venture Partners	$15,000,000
Aprio Technologies	DFM solutions for manufacturing processes	El Dorado Ventures/Goldman, Sachs & Co.	$14,725,200
Ecrio	Wireless messaging	DoCoMo Capital/Nexit Ventures Oy	$14,500,000
Oco	On-demand business intelligence	Highfields Capital Management/Individuals	$14,500,000
Sana Security	Network security market	Bay Partners/El Dorado Ventures	$14,362,000
Fabrik	Personal digital media application appliances	ComVentures/Intel Capital	$24,900,000
Beyond.com	Internet identity-mgt. tools	Safeguard Scientifics	$13,500,000
Arxan Technologies	Anti-tamper systems	EDF Ventures /Legend Ventures	$13,194,000
AirClic	Mobile information	JMI Equity/Motorola Ventures	$12,500,100
ViDeOnline Communications	Digital media distribution and access	Individuals/Intel Capital	$12,132,000
Black Duck Software	PrIP risk management and mitigation	Fidelity Ventures/Flagship Ventures	$12,000,200
Emergent Game Technologies	Software for online video gaming	Adena Ventures/Cisco Systems	$12,000,000
LeftHand Networks	Open iSCSI SANs.	Boulder Ventures/Garage Technology	$25,000,000
Ooma	Consumer voice applications market	Draper Fisher Jurvetson/Worldview Tech.	$12,000,000
ZenZui	Marketer-funded software on mobile devices	Hunt Ventures/Oak Investment Partners	$12,000,000
Fanfare Group	Testing of IP- based systems	Focus Ventures/Matrix Partners	$12,000,000
MaxiScale	Control of infrastructure costs	El Dorado Ventures/New Enterprise	$11,999,100
RingThree Technologies	Portable personal computing	Mohr Davidow Ventures/New Enterprise	$11,928,000
StreamBase Systems	Processing of streamed data	Accel Partners/Bessemer Venture Partners	$11,345,200
ForeScout Technologies	Clientless network access control	Accel Partners/Amadeus Capital Partners	$11,244,900
BayNote	Search and navigation engine technology	Chess Ventures/Hummer Winblad Venture	$10,750,000
Ocarina Networks	Storage and network subsystems	Highland Capital Partners/Kleiner Perkins	$10,548,000
VeraCode	Application security related products	406 Ventures	$19,500,000
Blaze DFM	Semiconductors	El Dorado Ventures/Lightspeed	$10,000,000
Cadent Holdings	3D digital information technology	Panorama Capital/Undisclosed firm	$10,000,000
ExaGrid Systems	Data protection and storage software	Highland Capital Partners/Undisclosed firm	$10,000,000
MyBuys	Web-based enterprise software applications	Lightspeed Venture Partners/Palomar	$9,498,000
Breach Security	Web application security	Enterprise Partners/Evergreen	$9,125,100
QuikCycle	Lab management and test automation	Crescendo Venture Management	$8,900,000
CoreObjects Software	Product development engine	Palomar Ventures	$8,500,000
Coghead	Web-based application creation	American Capital Strategies/El Dorado	$8,000,100
NewForma	Work process	North Bridge/Undisclosed Firm	$8,000,000
Construction Software Tech.	Web-based contracting	Chrysalis Ventures/Individuals	$7,929,000
Arcot Systems	User authentication and digital signing	Accel Partners/Goldman, Sachs & Co.	$7,870,200
Extreme DA	Semiconductor design tools	Foundation Capital/Individuals	$7,569,900
ClaraBridge	Unstructured data sources analysis	Boulder Ventures/Individuals	$7,500,000
Junction Solutions	Multi-channel retail and food and beverage	MK Capital	$7,500,000

services that are supposed to remediate whatever problems they find; I don't recommend using the accounting services however; I think you can obtain better results at a better price by using a third party for this phase of the process.)

Many of the second line accounting firms also supply audit services, often with a specific industry focus. Also, there are an increasing number of security and privacy management companies that address specific industries. One example is E3 Technologies; they do a lot of work for the financial industry. Audits from these companies can carry a great deal of weight with your customers but cost much less, ranging from $3k to $15k. But fixing problems can be expensive; count on spending an average of $50k to $100k to satisfy an audit's requirements. And once the audit is complete, you need to incorporate it directly into your sales cycle. Make sure it's packaged and readily available to your customers; your audit is going to be one of your most important pieces of sales support collateral during the buying cycle. I can guarantee that larger prospects will demand to see that audit before signing any checks.

> **"An interesting option that some SaaS firms are offering customers is a quick mirroring capability. This involves the ability almost immediately to transfer data and, in some cases, the entire SaaS application environment to the customer's infrastructure. In theory, this allows a SaaS consumer to avoid service interruptions with a minimum of time and agony.**
>
> *—John Shovic*
> *InstiComm*

Auditing companies always look for a layered approach to physical security. They're going to want to see:

- Secure facilities, including hardened server rooms, cages, controlled access, etc.
- Use of raid systems for local backup.
- Offsite backup capabilities (and their security abilities and privacy management abilities will also figure into the audit).
- Encryption built into the system at every point of communication, and device. This includes browsers, VPNs, PDAs, phone, USB ports, legacy ports, etc.

How important are SaaS escrow agreements?

Critical if you're going to be selling to larger or enterprise-class customers. They'll demand you have an escrow agreement in place before they'll do business with you. Also, big companies are going to want to see warranties in place; legal documents in which you guarantee service and performance.

Another point a SaaS provider should remember is that larger customers are going to want access to your financials. This can be a tough thing for a company to swallow, particularly if they're used to doing business in a licensed software environment. A company using a client server product installed on their internal servers doesn't normally worry that the software will stop working if your company stops operations. That's not the case in SaaS. Be prepared to provide access to your bottom line.

John C. Shovic, VP of business development, InstiComm, 610 W. Hubbard Ave., Ste. 124, Coeur d'Alene, Idaho, 83814; 208-292-1745. E-mail: john.shovic@insticomm.com.

Due Diligence: Get Ready to Meet the Buyer's Every Request

By Mark S. Reed, Corum Group

Due diligence is a buyer's detailed investigation into the affairs of your company before they acquire it. If you fail to prepare, you run the risk of destroying value and living with potential liability long after the deal is closed.

First, understand the scope of due diligence and prepare to satisfy the buyer's requests for information. Buyers want to know about a seller's financial, legal, operational and technical affairs, in other words "everything". The buyer's information request will be many pages long. Sellers should prepare well before the information is requested. Get a sample "due diligence checklist". Keep thorough and orderly records and document business processes so you can gather information when required. While this will be necessary for an acquisition, it is also a valuable discipline as your company grows.

Second, understand when to produce sensitive information. Buyers will ask for information about your customers, products, sales pipeline, financial statements, technology, and other aspects of your business. You need to disclose some information to assist the buyer in a purchase decision, but expect the buyer to show commitment to the transaction commensurate with the volume and sensitivity of information they request. Don't allow the buyer to ask for information without simultaneously requiring they dedicate equal effort to completing the transaction.

Third, remember that due diligence is about full disclosure. If your company has problems, face the facts, and plan how and when to disclose troublesome information to the buyer. Do this before a deal is negotiated. Time the delivery of bad news when you have the most leverage in negotiations. Your goal should be to ensure that the buyer has no surprises during due diligence. Undisclosed good news means you probably haven't captured full value for your company. Undisclosed bad news undermines your credibility and jeopardizes the transaction.

Fourth, in-depth due diligence is time consuming; begin this formal process only after the general terms of a transaction have been agreed to in writing, for example in a non-binding Letter of Intent (LOI). A seller should ask the buyer for a formal "due diligence checklist" immediately after executing an LOI.

Mark S. Reed, title, Corum Group, 10500 NE Eighth St., Bellevue, Wash. 98004; 425/455-8281. E-mail: mreed@corumgroup.com.

Company/Description	Acquired by	Price/Terms	Revenues	Multiple
Ceridian (CEN)	Thomas H. Lee Partners	$5,300,000,000	$1,590,000,000	**3.33**
• *Information management systems*		*Terms: Cash*		
Avaya (AV)	Silver Lake & TPG Capital	$8,200,000,000	$5,400,000,000	**1.52**
• *Communications Technologies*		*Terms: Cash*		
Krak (Denmark)	Eniro AB (Sweden) (ENIRF.PK)	$72,300,000	$35,400,000	**2.04**
• *Search and portal technologies*		*Terms: Cash*		
InfoGenesis	Agilysys (AGYS)	$90,000,000	$42,000,000	**2.14**
• *Point-of-sale products*		*Terms: Cash*		

CORUM
MERGERS & ACQUISITIONS

CardFile

Social Bookmarking Resources

- **BookmarkingDemon** (www.bookmarkingdemon.com): Desktop product that allows you to manage your social bookmarking placements and tagging.
- **egoSurf** (www.egosurf.com): Service allows you to search for sites linking to your blog and provides an "ego" ranking.
- **Open Tag Directory** (www.open-tag-directory.org): Useful directory of social bookmarking and blog sites.
- **Onlywire** (www.onlywire.com): System allows you to submit links to 17 social bookmarking sites simultaneously.
- **Social Bookmarks Creator** (www.toprankblog.com/tools/social-bookmarks): Fee online tool that creates social bookmarking links for your website; can create both links and drop down menus.
- **TagJag** (www.tagjag.com): Website allows you search a wide variety of blogs, social bookmarking sites, and RSS feeds by keywords (tags).

ZDNET BLOGGER JOE WILCOX ON SYNCHRONIZATION: "If Google gets synchronization right before Microsoft, it's game over. Google would be able to extend the relevancy of the Web platform back to the desktop on its terms; think invading army. If Microsoft gets synch right, it can drive desktop relevancy the other way, invading Google turf. Microsoft missed a huge opportunity by failing to deliver synchronization as a core Windows Vista service." (Quoted on http://www.microsoft-watch.com, 06/06/2007)

ZDNET BLOGGER ED BOTT ON BUNDLING WINDOWS WITH MACS: "So, my prediction: Come October, when Leopard ships, Apple will announce that anyone buying a new Mac can order an Apple-customized version of Windows Vista preinstalled on the same system." (Quoted on http://blogs.zdnet.com/Bott/?p=255&tag=nl.e539, 06/12/2007)

REPORTER STRUAN ROBERTSON ON THE LAW AND GOOGLE STREET VIEW IN EUROPE: "Our data protection regime lets us take holiday snaps, even of strangers, provided we're doing so for private purposes. But if we're taking snaps for commercial use, where individuals are identifiable, there is no such exemption." (Quoted on http://www.theregister.com, 06/05/2007)

GOOGLE WATCHER DANNY SULLIVAN ON GOOGLE'S RECENT POOR PRIVACY RATINGS: "It's a bad privacy day for Google, with Privacy International first accusing the company of having the worst privacy performance of any internet service company in a study it has just released and then accusing Google of conducting a smear campaign against it. But if you actually read the report, Privacy International itself comes off bad for putting out a haphazard condemnation of Google." (Quoted on http://searchengineland.com/070610-100246.php, 06/10/2007)

Colleagues made off with your last issue? Go to www.softletter.com. Click Subscriber Login in the upper right of the home page. To view the current issue and to search archives of hundreds of articles by keyword, topic, or issue date, log in and enjoy!

Soft•letter is published 24 times per year; entire contents copyright © 2007 by Soft•letter. All rights reserved. Reproduction by any means, without permission of the publisher, is prohibited. ISSN: 0882-3499.

Subscription rates: $395 worldwide. Subscription office:
Aegis Resources
34 Sugar Hill Rd.
Killingworth, Conn. 06419
Voice:860/663-0552
Fax: 860/663-0553
info@softletter.com

www.softletter.com