

2012 Outlook for Company Start Ups

Prepared by Scott H Leonard

Annually, I review various changes in technology, software, security, and marketing, while exploring the playing field of Company Start Ups for 2012. It is not intended to predict events in the upcoming year, but to examine current developments as we look towards the next 12 months.

In review of things past and things to come, this year my focus seems to be on the fast paced launch of companies, brands, and products, while overlooking impending security threats.

In the last 24 months, technology has advanced at light-speed. Years ago, a company would go into business with a 4 year break even goal. Today, companies are going all-in to launch themselves, their brand, or their product with a 90 to 180 day break even goal! They are literally putting it all on the line with a pull-the-plug plan in place if goals are not reached in the short term. Their mindset is simple. It is better to swallow your loss and regroup, then to wade through 4 years of failure. A high-level approach to “throw spaghetti on the wall to see if it sticks.”

Industry consultants and marketing experts are split. Some are old-school and believe you should stuff their pockets for 12 months of research and preparation, then dig in and work towards the 4 year mark. Others are sitting on extraordinary technologies, software, and marketing channels. The approach of these elite specialists is to empower you to take action and position yourself, before your competition does.

I spoke of it as we entered 2011, never before has it been possible to establish 90-180 day goals for business. In 2012, you will see more and more of these short-term business models. Slowly, people are able to tap true viral marketing. No need to mention the Viral Marketing model was taught 15 years ago... people are only now able to engage in it.

With advancements in technology and penetration of user markets, I must take a moment to discuss security issues ignored. In my opinion, instant success in 2012 will be met with instant failure due to ignored risks which are prevalent.

Q: If I sit at your laptop... must I enter a password to use it?

NOTE: 8 out of 10 people have no password to use computer.

A Coffee Shop thief has an 80% opportunity for success!

Q: Can I access your web-based email without entering a Username and Password?

NOTE: 6 out of 10 people check a box “Save my Password” which allows them to return to the page and login, without entering a username or password.

Hmmmm, Email, Bank, Stocks, VPN, FTP Program, Yahoo Messenger, SKYPE, Google...

If someone sat at your computer... how much of your life could be stolen, in seconds?

Q: Can I open and use your Mobile without a password?

NOTE: 9 out of 10 people do not use this password feature on their mobile phone.

As we enter 2012, we MUST change how we handle our technology. Technology is advancing quickly, hackers are advancing quickly, our disposable nature is advancing quickly... a Train Wreck is on the Horizon.

1.) In-Person / Insider threats are of first concern.

An open laptop or desktop provides instant and easy access to a wealth of private data. Many people check a box during logins which saves username and password in order to instantly login when you return. Imagine; your bank or stock account, emails, messengers (MSN, Skype, Yahoo), Social Network Logins (FaceBook,

Twitter, MySpace, etc). In a matter of seconds an attempt to login to your bank account or other services, do a password reset, open your email to confirm reset and i have private access to your bank, social networks, and other services, then delete the emails. I could have added my email to the account and confirmed as well. Now on my computer, I go to work, stealing your money, your identity, your contacts, or outright ruin your reputation and connections in social networks. It is hard to undo, once started. And since it begins from your computer and was email verified via your email, I have a head start with full authority as if I am you.

Unfortunately, you probably won't recognize the breach for days.

This is the first and most serious security breach.

2.) Spam

Short of being in person at your computer, spam represents a barrage of attempts to get your attention with a 'slight of hand' and goal to penetrate. Some to penetrate your wallet and get you to buy something, but mostly to simply 'get in.'. Generally under estimated, spam serves as a vehicle for a plethora of security breaches.

The spam threat continues to rise causing email hosts to ramp up filtering algorithms. Just this week I spoke with a client that had about 700 of 800 emails bounce that he regularly sends to. In his case, he began offering an online prescription drug discount service. He is a legitimate company, but his recent newsletter was probably blocked by text within.

Many spam emails get through, but heightened security has a draw back of some good email being canned.

Common flagged words are: prescription, drug, Viagra, weight loss, enhancement, MLM, opportunity.

Every email company runs their own algorithm, so they vary.

I shared this to impress on you the seriousness of spam and how it is aggressively on the radar of technology experts as an extreme security threat. They continue to monitor and adjust their algorithms reducing what you actually receive. That said, the greatest risk may be those that avoid the algorithm and appear in your email.

3.) Malware

To some degree, malware is more often the result of the wrong mouse click. An instant message or email from a friend carries a hyperlink and looks sincere, a spam email doesn't look like spam and the subject looks enticing, an email attachment or a website built to spawn the malware.

What is malware? It is a global term for programs that are malicious. Viruses, worms, Trojans, spyware, browser hijacks, adware, keyword loggers and more.

Occurrences have dropped slightly, but damage more severe. We may attribute changes in every area if technology to the slight drop; firewall updates, spam algorithms, intelligent warnings of operating system when attempts to install occur, increased network security, fewer potential exploits of operating systems.

Ultimately, it just means that criminals have to hone their skills and dig deeper.

The threat of malware is serious. It is the unwary click of a user that often triggers the silent but serious threat.

As a side note, hackers are also advancing with technology. 10 years ago I had a sweet portal-based website. Smooth and flawless for 5 years, then a note in the footer... 'you have been hacked'. It floored me as I knew the security built in the system. The point, continued advancements in hacker skills require continued advancements in security and protective measures. In retrospect, I was very fortunate to have gone five years with ZERO code or security updates. This example was not malware but goes to show that security measures must continue to advance. We can not sit idle and expect our current measures to be adequate in the future.

4.) External Intruders

Malware, mentioned above, can be an autonomous program sent to do a job, or to pass data out, or to open a door in. It's not the only way in though. Once in, it's like me sitting at your computer, the sky is the limit. Literally, an area can be partitioned on your hard drive to perform any task, from recording of user input,

duplication of files, even operating a program from your hard drive that accesses the web to further spread it's maliciousness through your contacts, or outright conducts illegal activity. I am an individual whose computer was engaged in selling pornography, leading to law enforcement entering his office and seizing his computer. The his name was damaged and he risked jail... fortunately, some of the dates and times of the transactions coincided with times which he had visited the state house, signing a roster as he entered. I mentioned this event, as it was a horrible ordeal for the individual, yet was an automated software/script that apparently gained access to his computer via an in-bound email. Once in, it took on a life of it's own, making money for someone, while placing the risk on another!

5.) Pharming or Phishing Attacks

Generally, users are unaware of the Pharming or Phishing Attacks, falling quickly into the snare. A common one would be a generic email from a respected website, such as a Bank or maybe Paypal, with a notice... "We have enhanced our security system and require that you login to confirm your email address again," or to answer a series of questions, etc. Seldom do users recognize the page they clicked over to has a web address similar to the correct site, but NOT! They prepared the page to look very similar to the real site and as a user, you willingly enter your username and password.... Captured! A well planned Pharming or Phishing Attack can encourage ten's of thousands of users to willingly navigate to a page and enter their personal login credentials.

6.) Servers, Hardware, and Operating Systems

We went through an era of Physical Servers to Virtual Servers to Cloud Servers. In order to reduce risk and liability to these systems, limited information has hit the streets, in the area of their security risks. When Cloud Computing began, there was a great deal of 'Small Talk' on various concerns and risks, but IT managers are actively engaged in securing server infrastructures and reducing their risks by not discussing obvious concerns.

Operating Systems are at the forefront, however many pieces of hardware are now involved in the operation of a website, each of which often have an operating system or some form of software running it. This has created multiple layers of security concerns. In general, I have a preference to Windows Systems. They are under the most fire by hackers, but they are also under the most advancement. Other operating system, including open-source systems, are limited to the programmer of the software application or website. To his skills and talents in creating and managing security routines. Couple server OS risks with the firmware of your firewall and other hardware systems, you will quickly be lost in extreme potentials of risk, especially if you are operating a website that stores personal data. Today, it is not particularly reasonable to attempt to host your systems on in-office, as constant management of security risks can put you under. It is more reasonable to expect a strategic alliance with a hosting facility to manage hardware and security on that side. (Not your application security)

7.) Peripherals

2011 ushered in a new era of peripheral devices that are being treated as disposable. iPhone and iPad have very little upgrade capability, permitting the company to market to existing users, their next generation of product. Never before have we owned so many mobile and tablet devices and been so readily willing to buy the next one that comes out. There are two primary categories of Peripherals, Currently Used and Ignored or Lost. Both have basically the same risks, only one is currently with you and the other disregarded. Recent information has hit the streets of programs operating on the devices which track and log everything you do... and I mean everything. The individual bringing this information to light has been under tremendous attack and lawsuits, as companies try to keep this quiet. Strangely, the data being tracked is a third party of the mobile device and there is no knowledge of what the data is being used for. That is serious, considering you log into your Bank Account, Stock Portfolio, VPN, Emails, and much more. This is an extremely high risk area that we continue to engage in every day. Some phones have offered the user to turn off local tracking so the Default Method of storing your Location with every photo is turned off. That said, these other programs still track and store.

Now, consider that ignored device... Where is it? What is on it? Who has it? "A Hammer comes to mind!"

8.) Outsourcing

I truly hate to mention this one, but someone must do it. Mobile Phone Providers, Banks, Software Providers, and even Credit Bureaus are outsourcing their Customer Support!

Think: SSN, Date of Birth, Name, Address, City, State, Zip, Phone, Email.

These are the items that can be used to ruin your life, as someone establishes their new identity with yours. I can understand outsourcing customer support of user functions within a web-based system, but when outsourced customer support reps have access to your back office, or to your personal information, something is wrong.

My Personal Experience: I attempted to log into one of the 3 credit bureaus to check my credit report. It asked a series of security questions that I did not recognize. When I called Customer Support to get logged in, I was speaking with a representative in India. When the representative asked for my Social Security Number and Date of Birth, I fell out of my chair! Why, would our credit bureaus EVER outsource? WHY? Credit Bureaus, Banks, on line eCommerce Sites... they all have one thing in common. A desire to provide affordable customer services, while handling YOUR personal data.

Let's get a handle on security as we build success in 2012.

Marketing

For 2012, companies must get honest with themselves what they are in business to do. It is not to get rich, or to have 1 million customers. It is to Sell a particular product or product line, for a profit.

In order to be successful in 2012, we must be clear about what we are selling and be passionate in our pursuit and propagation of the benefits of our products and services.

Engaging in email campaigns will be more and more risky, and less and less profitable.

Amazon.com is most effective for direct sales of a product, linked back to your company for upsells.

Relevant advertising in Google and Bing are most effective for online direct advertising of a company's products and services.

Facebook and Twitter are most effective for secondary marketing through social channels.

LinkedIn and YouTube are most effective for establishing Branding when done right.

Direct Selling through a Network Marketing Sales Channel (MLM) is most effective for penetrating a market with your message and for sales.

Sincerely,

Scott H Leonard

1-888-221-0106

616-770-7107

<http://mlmsoftwarecentral.com/>

About the Author: Scott H Leonard has been actively engaged in both the business and personal computer and technologies industries for over 17 years. Providing consulting, marketing, software development, ecommerce, website design, hosting, domain and other services to business and consumers through his personal and privately owned, BizLocal Technologies. Several projects have sought to provide security to personal computers, limit risk and exposure of children going online, tracking child usage, controlling site access, and prevention of key logging or data capture.