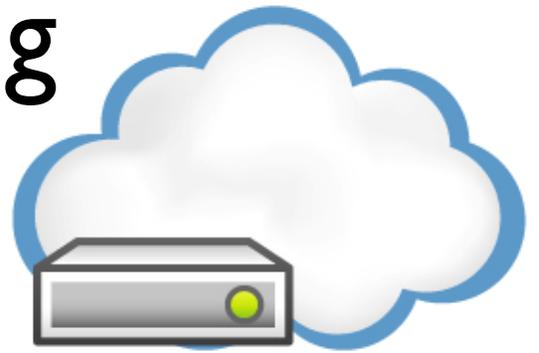# INTRO TO CLOUD COMPUTING

"5 Critical Facts Every Business Owner Must Know Before Moving Their Network To The Cloud"

Discover What Most IT Consultants Don't Know Or Won't Tell You About Moving Your Company's Network To The Cloud

By: Yigal Behar
www.2Secure.biz
Tel: 646-755-3933

A Letter From The Author:
Why We Created This Report And Who Should Read It

From The Desk of: Yigal Behar
CEO, 2Secure Corp

Dear Colleague,

When you decided to look into transitioning your computer network and operations to the cloud, you were probably met with conflicting advice, confusion and no real answers to your questions and concerns over security, cost and whether or not it's appropriate for your organization.

That's why we wrote this report. **We wanted to give CEOs and business leaders a simple, straightforward guide that not only answers your questions in plain English, but also provides vital experience-based information that most IT companies don't know (or may not tell you) that could turn your migration into a big, cash-draining nightmare.**

My name is Yigal Behar My organization has been working for the past 13 years in Cybersecurity. The cloud revolution has brought many good improvements to business around the world. This change has a great privacy and safety impact. As it turns out, using cloud solutions will increase costs when a Security breach has identified.

The simple fact is, cloud computing is NOT a good fit for every company, and if you don't get all the facts or fully understand the pros and cons, you can end up making some VERY poor and expensive decisions that you'll deeply regret later. The information in this report will arm you with the critical facts you need to avoid expensive, time-consuming mistakes.

Of course, we are always available as a resource for a second opinion or quick question, so please feel free to contact my office direct if we can clarify any points made in this report or answer any questions you have.

Dedicated to serving you,

Yigal Behar – CEO

2Secure Corp

5 Critical Facts You Must Know
Before Moving To The Cloud

In this report I'm going to talk about **5 very important facts you need to know before you consider cloud computing for your company**. These include:

1. The pros AND cons you need to consider before moving to the cloud.
2. Migration GOTCHAS (and how to avoid them).
3. The various types of cloud computing options you have (there are more than just one).
4. Answers to important, frequently asked questions you need to know the answers to.
5. What questions you need to ask your IT pro before letting them "sell" you on moving all or part of your network and applications to the cloud.

I've also included some actual case studies from other businesses that have moved to cloud computing, along with a sample cost-comparison chart so you can see the impact this new technology can have on your IT budget.

At the end of this report there is an invitation for you to request a **Free Cloud Readiness Assessment** to determine if cloud computing is right for your particular business. I encourage you to take advantage of this before making any decisions since we've designed it to take a hard look at the functionality and costs for you as a business and provide you with the specific information you need (not hype) to make a good decision about this new technology.

What Is Cloud Computing?

Wikipedia defines cloud computing as "the use and access of multiple server-based computational resources via a digital network (WAN, Internet connection using the World Wide Web, etc.)."

But what the heck does *that* mean?

The easiest way to not only understand what cloud computing is but also gain insight into why it's gaining in popularity is to compare it to the evolution of public utilities. For example, let's look at the evolution of electricity.

Back in the industrial age, factories had to produce their own power in order to run machines that produced the hard goods they manufactured. Be it textiles or railroad spikes, using machines gave these companies enormous competitive advantages by producing more goods with fewer workers and in less time. For many years, the production of power was every bit as important to their company's success as the skill of their workers and quality of their products.

Unfortunately, this put factories into TWO businesses: the business of producing their goods and the business of producing power. Then the concept of delivering power (electricity) as a utility was introduced by Thomas Edison when he developed a commercial-grade replacement

464 Kings Highway 2nd, Floor, NY 11223 | www.2secure.biz | Tel: 646-755-3933

for gas lighting and heating using centrally generated and distributed electricity. From there, as they say, the rest was history.

The concept of electric current being generated in central power plants and delivered to factories as a utility caught on fast. This meant manufacturers no longer had to be in the business of producing their own power with enormous and expensive water wheels. **In fact, in a very short period of time, it became a competitive necessity for factories to take advantage of the lower-cost option being offered by public utilities.** Almost overnight, thousands of steam engines and electric generators were rendered obsolete and left to rust next to the factories they used to power.

What made this possible was a series of inventions and scientific breakthroughs – but what drove the demand was pure economics. Utility companies were able to leverage economies of scale that single manufacturing plants simply couldn't match in output or in price. In fact, the price of power dropped so significantly that it quickly became affordable for not only factories but every single household in the country.

Today, we are in a similar transformation following a similar course. The only difference is that instead of cheap and plentiful electricity, advancements in technology and Internet connectivity are driving down the costs of computing power. With cloud computing, businesses can pay for "computing power" like a utility without having the exorbitant costs of installing, hosting and supporting it on premise.

In fact, you are probably already experiencing the benefits of cloud computing in some way but hadn't realized it. Below are a number of cloud computing applications, also called SaaS or "software as a service," you might be using:

- Gmail, Hotmail or other free e-mail accounts
- Facebook
- NetSuite, Salesforce
- Constant Contact, Exact Target, AWeber or other e-mail broadcasting services
- Zoomerang, SurveyMonkey and other survey tools
- LinkedIn
- Twitter
- All things Google (search, AdWords, maps, etc.)
- Amazon AWS
- Microsoft Azure

If you think about it, almost every single application you use today can be (or already is) being put "in the cloud" where you can access it and pay for it via your browser for a monthly fee or utility pricing. You don't purchase and install software but instead access it via an Internet browser.

What About Office 365 And Google Apps?

Office 365 and Google Apps are perfect examples of the cloud computing trend; for an inexpensive monthly fee, you can get full access and use of Office applications that used to cost a few hundred dollars to purchase. And, since these apps are being powered by the cloud provider, you don't need an expensive desktop with lots of power to use them – just a simple Internet connection will do on a laptop, desktop or tablet.

Pros And Cons Of Moving To The Cloud

As you read this section, keep in mind there is no "perfect" solution. All options – be it an in-house, on-premise server or a cloud solution – have upsides and downsides that need to be evaluated on a case-by-case scenario. (Warning: Do NOT let a cloud expert tell you there is only "one way" of doing something!)

Keep in mind the best option for you may be a **hybrid solution** where some of your applications and functionality are in the cloud and some are still hosted and maintained from an in-house server. We'll discuss more of this in a later section; however, here are some general pros and cons of cloud computing:

Pros Of Cloud Computing:

- **Lowered IT costs.** This is probably the single most compelling reason why companies choose to move their network (all or in part) to the cloud. Not only do you save money on software licenses, but on hardware (servers and workstations) as well as on IT support and upgrades. So if you hate constantly writing cash-flow-draining checks for IT upgrades, you'll really want to look into cloud computing.

- **Ability to access your applications and data from anywhere and any device.** If you travel a lot, have remote workers or prefer to use an iPad while traveling and a laptop at your house, cloud computing will give you the ability to work from any of these devices.

- **Disaster recovery and backup are automated.** The server in your office is extremely vulnerable to a number of threats, including viruses, human error, hardware failure, software corruption and, of course, physical damage due to a fire, flood or other natural disaster. If your server were in the cloud and (God forbid) your office was reduced to a pile of rubble, you could purchase a new laptop and be back up and running within the same day. This would NOT be the case if you had a traditional network and were using tape drives, CDs, USB drives or other physical storage devices to back up your system.

  Plus, like a public utility, cloud platforms are far more robust and secure than your average business network because they can utilize economies of scale to invest heavily into security, redundancy and failover systems, making them far less likely to go down.

- **It's faster, cheaper and easier to set up new employees.** If you have a seasonal workforce or a lot of turnover, cloud computing will not only lower your costs of setting up new accounts, but it will make it infinitely faster.

- **You use it without having to "own" it.** More specifically, you don't own the *responsibility* of having to install, update and maintain the infrastructure. Think of it as similar to living in a condo where someone else takes care of the building maintenance, repairing the roof and mowing the lawn, but you still have the only key to your section of the building and use of all the facilities. This is particularly attractive for companies that are new or expanding, but don't want the heavy outlay of cash for purchasing and supporting an expensive computer network.

- **It's a "greener" technology that will save on power and your electric bill.** For some smaller companies, the power savings will be too small to measure. However, for larger companies with multiple servers that are cooling a hot server room and keep their servers running 24/7/365, the savings are considerable.

Cons Of Cloud Computing:

- **The Internet going down.** While you can mitigate this risk by using a commercial-grade Internet connection and maintaining a second backup connection, there is a chance you'll lose Internet connectivity, making it impossible to work.

- **The cloud service going down:** in the past we have seen google, office365 and Amazon are going down or slowing down; like you they have some issues; power, employees and other operational issues that can cause a service interruption, therefore don't have all eggs in one nest.

- **Where is my data?** Many people don't feel comfortable having their data in some off-site location. This is a valid concern, and before you choose any cloud provider, you need to find out more information about where they are storing your data, how it's encrypted, who has access and how you can get it back. You'll find more information on this under "What To Look For When Hiring A Cloud Integrator" later on in this document. As it sounds "Cloud" means my data can be "traveling" on the wire to anywhere in the world. This done for the sake of cost reduction and backup or as redundant site and is not something you, as the owner of the data can have control over.

- **What type of data will be saved?** Data types can include intellectual property, personal information that contains social security, credit card numbers or maybe medical information. You need to decide what information should be stored in the cloud.

- **Who has access to my data?** Since the information and applications are served from the "cloud" anyone that sits in the cloud may have access. What security controls the cloud provider has enforced protecting your data and how can you influence that.

- **Can my data leaks from my systems to other systems?** Your data can leak from your cloud systems to another system in the cloud, it is possible when different systems are

464 Kings Highway 2nd, Floor, NY 11223 | www.2secure.biz | Tel: 646-755-3933

joined together to ease management tasks and costs. You should ask the provider how and what controls are used to maintain data and applications separation.

- **How will my internal applications be interacting with my cloud applications?** In today's varies applications and systems are interconnecting with other systems for data exchange, for instance accounting systems is getting its data from client management software for billing, how this move to the cloud will affect my business.

- **Compliance Issues.** There are a number of laws and regulations, such as Gramm-Leach-Bliley, Sarbanes-Oxley and HIPAA and PCI-DSS that require companies to control and protect their data and certify that they have knowledge and control over who can access the data, who sees it and how and where it is stored. In a public cloud environment, this can be a problem. Many cloud providers won't tell you specifically where your data is stored.

  Most cloud providers have SAS 70 certifications, which require them to be able to describe exactly what is happening in their environment, how and where the data comes in, what the provider does with it and what controls are in place over the access to and processing of the data; but as the business owner, it's YOUR neck on the line if the data is compromised, so it's important that you ask for some type of validation that they are meeting the various compliance regulations on an ongoing basis. It is recommended that you will have the right to bring a 3rd party for auditing their systems.

464 Kings Highway 2nd, Floor, NY 11223 | www.2secure.biz | Tel: 646-755-3933

Migration Gotchas! What You Need To Know About Transitioning To A Cloud-Based Network

When done right, a migration to Office 365 or another cloud solution should be like any other migration. There's planning that needs to be done, prerequisites that have to be determined and the inevitable "quirks" that need to be ironed out once you make the move.

Every company has its own unique environment, so it's practically impossible to try and plan for every potential pitfall; however, here are some BIG things you want to ask your IT consultant about BEFORE making the leap.

Downtime. Some organizations cannot afford ANY downtime, while others can do without their network for a day or two. Make sure you communicate YOUR specific needs regarding downtime and make sure your IT provider has a solid plan to prevent extended downtime.

Painfully Slow Performance. Ask your IT consultant if there's any way you can run your network in a test environment before making the full migration. Imagine how frustrated you would be if you migrate your network and discover everything is running so slow you can barely work! Again, every environment is slightly different, so it's best to test before you transition.

3rd-Party Applications. If your organization has plug-ins to Exchange for faxing, voice mail or integration into another application, make sure you test to see if it will still work in the new environment.

Different Types Of Cloud Solutions Explained:

Pure Cloud: This is where all your applications and data are put on the other side of the firewall (in the cloud) and accessed through various devices (laptops, desktops, iPads, phones) via the Internet.

Hybrid Cloud: Although "pure" cloud computing has valid applications, for many it's downright scary. And in some cases it is NOT the smartest move, due to compliance issues, security restrictions, speed and performance. A hybrid cloud enables you to put certain pieces of existing IT infrastructure (say, storage and e-mail) in the cloud, and the remainder of the IT infrastructure stays on-premises. This gives you the ability to enjoy the cost savings and benefits of cloud computing where it makes the most sense without risking your entire environment.

Single Point Solutions: Another option would be to simply put certain applications, like SharePoint or Microsoft Exchange, in the cloud while keeping everything else on-site. Since e-mail is usually a critical application that everyone needs and wants access to on the road and on various devices (iPad, smartphone, etc.), often this is a great way to get advanced features of Microsoft Exchange without the cost of installing and supporting your own in-house Exchange server.

Public Cloud Vs. Private Cloud: A public cloud is a service that anyone can tap into with a network connection and a credit card. They are shared infrastructures that allow you to pay-as-you-go and are managed through a self-service web portal. Private clouds are essentially self-built infrastructures that mimic public cloud services, but are on-premises. Private clouds are often the choice of companies who want the benefits of cloud computing, but don't want their data held in a public environment.

464 Kings Highway 2nd, Floor, NY 11223 | www.2secure.biz | Tel: 646-755-3933

FAQs About Security, Where Your Data Is Held
And Internet Connectivity

Question: How long will it take to transition my on-premises server to the cloud, and what's the process?

Answer: depending on your existing applications, data, amount of users, locations it can take from a week to 30 days.

Question: What if my Internet connection goes down? How will we be able to work?

Answer: While this is a valid concern, we overcome it in the following way for our clients in the cloud. Install 2nd Internet connection from another company and some cases using 3G/4G wireless connectivity. There is always the option to work from home or a coffee shop.

Question: What happens if the Internet slows to the point where it's difficult to work productively?

Answer: We resolve this by keeping a synchronized copy of your data on your on-site server as well as in the cloud. Here's how this works: Microsoft offers a feature with Windows called "DFS," which stands for Distributed File Systems. This technology synchronizes documents between cloud servers and local servers in your office. So instead of getting rid of your old server, we keep it on-site and maintain an up-to-date synched copy of your files, folders and documents on it. If the Internet goes down or slows to a grind, you simply open a generic folder on your PC and the system will automatically know to pull the documents from the fastest location (be it the cloud server or the local one). Once a file is modified, it syncs it in seconds so you don't have to worry about having multiple versions of the same document. Using this process, you get the benefits of cloud with a backup solution to keep you up and running during slow periods or complete Internet outages.

Another option could be adding another Internet provider balancing traffic to both Internet connections.

Question: What about security? Isn't there a big risk of someone accessing my data if it's in the cloud?

Answer: In many cases, cloud computing is a MORE secure way of accessing and storing data. Just because your server is on-site doesn't make it more secure; in fact, most small to medium businesses can't justify the cost of securing their network the way a cloud provider can. And most security breaches occur due to human error – one of your employees downloads a file that contains a virus, they don't use secure passwords or they simply e-mail confidential information out to people who shouldn't see it. Other security breaches occur in on-site networks because the

464 Kings Highway 2nd, Floor, NY 11223 | www.2secure.biz | Tel: 646-755-3933

company didn't properly maintain their own in-house network with security updates, software patches and up-to-date antivirus software. That's a FAR more common way networks get compromised versus a cloud provider getting hacked.

Question: Do I have to purchase new hardware (servers, workstations) to move to the cloud?

Answer: No! That's one of the selling points of cloud computing. It allows you to use older workstations, laptops and servers because the computing power is in the cloud. Not only does that allow you to keep and use hardware longer, but it allows you to buy cheaper workstations and laptops because you don't need the expensive computing power required in the past.

What To Look For When Hiring An IT Consultant To Move Your Network To The Cloud

Unfortunately, the IT consulting industry (along with many others) has its own share of incompetent or unethical people who will try to take advantage of trusting business owners who simply do not have the ability to determine whether or not they know what they are doing. Sometimes this is out of greed for your money; more often it's simply because they don't have the skills and competency to do the job right but won't tell you that up front because they want to make the sale.

From misleading information, unqualified technicians and poor management, to terrible customer service, we've seen it all, and we know they exist in abundance because we have had a number of customers come to us to clean up the disasters they have caused.

Automotive repair shops, electricians, plumbers, lawyers, realtors, dentists, doctors, accountants, etc., are heavily regulated to protect the consumer from receiving substandard work or getting ripped off. However, the computer industry is still highly unregulated and there are few laws in existence to protect the consumer – **which is why it's so important for you to really research the company or person you are considering, to make sure they have the experience to set up, migrate and support your network to the cloud.**

Anyone who can hang out a shingle can promote themselves as a "cloud expert." Even if they are honestly *trying* to do a good job for you, their inexperience can cost you dearly in your network's speed and performance or in lost or corrupt data files. To that end, here are 7 questions you should ask your IT person before letting them migrate your network to the cloud:

Critical Questions To Ask Your IT Company Or Computer Consultant BEFORE Letting Them Move Your Network To The Cloud (Or Touch Your Network!)

Question: How many clients have you provided cloud services for to date and can you provide references?

Answer: You don't want someone practicing on your network. At a minimum, make sure they have few clients you speak.

Question: How quickly do they guarantee to have a technician working on an outage or other problem?

Answer: Anyone you pay to support your network should give you a written SLA (service level agreement) that outlines exactly how IT issues get resolved and in what time frame. I would also request that they reveal what their average resolution time has been with current clients over the last three to six months.

They should also answer their phones live from 8:00 a.m. to 5:00 p.m. and provide you with an emergency after-hours number you may call if a problem arises, including on weekends.

If you cannot access your network because the Internet is down or due to some other problem, you can't be waiting around for hours for someone to call you back OR (more importantly) start working on resolving the issue. Make sure you get this in writing; often cheaper or less experienced consultants won't have this or will try and convince you it's not important or that they can't do this. Don't buy that excuse! They are in the business of providing IT support, so they should have some guarantees or standards around this they share with you.

Question: Where will your data be stored?

Answer: You should receive full documentation about where your data is, how it's being secured and backed up and how you could get access to it if necessary WITHOUT going through your provider. Essentially, you don't want your cloud provider to be able to hold your data (and your company) hostage.

Question: How will your data be secured and backed up?

Answer: If they tell you that your data will be stored in their own co-lo in the back of their office, what happens if THEY get destroyed by a fire, flood or other disaster? What are they doing to secure the office and access? Are they backing it up somewhere else? Make sure they are SAS 70 certified and have a failover plan in place to ensure continuous service in the event

464 Kings Highway 2nd, Floor, NY 11223 | www.2secure.biz | Tel: 646-755-3933

that their location goes down. If they are building on another platform, you still want to find out where your data is and how it's being backed up.

Question: Do they have adequate errors-and-omissions insurance as well as workers' compensation insurance to protect YOU?

Answer: Here's something to consider: if THEY cause a problem with your network that causes you to be down for hours or days or to lose data, who's responsible? Here's another question to consider: if one of their technicians gets hurt at your office, who's paying? In this litigious society we live in, you better make darn sure that whomever you hire is adequately insured with both errors-and-omissions insurance AND workers' compensation – and don't be shy about asking to see their latest insurance policies!

True Story: A few years ago Geek Squad was slapped with multimillion-dollar lawsuits from customers for the bad behavior of their technicians. In some cases, their techs were accessing, copying and distributing personal information they gained access to on customers' PCs and laptops brought in for repairs. In other cases, they lost clients' laptops (and subsequently all the data on them) and tried to cover it up. Bottom line: Make sure the company you are hiring has proper insurance to protect YOU.

Question: Is it standard procedure for them to provide you with written network documentation detailing what software licenses you own, your critical passwords, user information, hardware inventory, etc., or are they the only person with the "keys to the kingdom"?

Answer: You should NEVER allow an IT person to have that much control over you and your company. If you get the sneaking suspicion that your current IT person is keeping this under their control as a means of job security, get rid of them (and we can help to make sure you don't suffer ANY ill effects). This is downright unethical and dangerous to your organization, so don't tolerate it!

Question: Do they INSIST on doing periodical test restores of your backups to make sure the data is not corrupt and could be restored in the event of a disaster?

Answer: Perform a monthly "fire drill" and perform a test restore from backups to make sure data CAN be recovered in the event of an emergency. After all, the WORST time to "test" a backup is when you desperately need it.

Free Assessment Shows You How To Migrate To The Cloud And Avoid Overpaying For Your Next IT Project Or Upgrade

If you're like a number of CEOs we've helped, you've already been burned, disappointed and frustrated by the questionable advice and **complete lack of service** you've gotten from other IT companies. In fact, you might be so fed up and disgusted from being "sold" that you don't trust anyone. *I don't blame you*.

That's why I'd like to offer you a **FREE Cloud Readiness Assessment** to show you there IS a better way to upgrade your computer network AND to demonstrate how a truly competent IT consultant (not just a computer "mechanic") can guide your company to greater profits and efficiencies, help you be more strategic and give you the tools and systems to fuel growth.

At no cost or obligation, one of my lead consultants and I will come to your office and conduct a thorough review and inventory of your current computer network, backups and technologies to give you straightforward answers to the following:

- ✓ How using cloud technologies may be able to eliminate the cost, complexity and problems of managing your own in-house server while giving you more freedom, lowered costs, tighter security and instant disaster recovery. I say "may" because it might NOT be the best choice for you. I'll give you honest answers to your questions and detail – in plain English – the pros AND cons of moving your specific operations to the cloud.

- ✓ Are your IT systems truly safe and secured from hackers, viruses and rogue employees? (FACT: 99% of the computer networks we review are NOT, much to the surprise of the CEOs who are paying some other "so-called" expert to manage that aspect of their IT.)

- ✓ Are your backups configured properly to ensure that you could be back up and running again fast in a disaster? From our experience, most companies' backups are an epic waste of money and only deliver a false sense of security.

- ✓ If you are ALREADY using "cloud" technologies, are you adequately protecting your organization from the dozens of ways you and your organization can be harmed, sued or financially devastated due to security leaks, theft, data loss, hacks and violating ever-expanding data privacy laws?

Even if you decide not to move your network to the cloud or engage with us as a client, you'll find the information we share with you to be extremely valuable and eye-opening when you make future decisions about IT. After all, it NEVER hurts to get a third-party "checkup" of your IT systems' security, backups and stability, as well as a competitive cost analysis.

There Is One Small "Catch"

Because our Cloud Readiness Assessments take between five and seven hours to complete (with most of this "behind-the-scenes" diagnostics and research we conduct), I can only extend this offer to the first seven people who respond. After that, we'll have to withdraw this offer or ask that you pay our customary consulting fee of $350 for this Assessment (sorry, no exceptions).

To respond, please call our office at 646-755-3933 and ask for me, Yigal. I personally want to take your call to answer any questions about this letter, my company and how we might be able to help you, CEO to CEO. You can also e-mail me direct at Yigal@2Secure.biz

Awaiting your response,

Yigal Behar
www.2Secure.biz
Call us direct: 646-755-3933

The Top 8 Reasons Why You'll Want To Outsource Your IT Security Operations To Us:

While we don't always observe this when we look at other security consulting firms, this is what we feel should be part of your service:

1. **We Care.** We treat your network as if it was our own. We protect your data as if it was ours. Your financial considerations are ours, well; we won't ask you to spend more than what is required.

2. **We Respond Within 15 Minutes Or Less.** The average amount of time it takes for one of our clients to get on the phone with a technician who can start working on resolving your problem is 10 minutes. We know you're busy and have made a sincere commitment to making sure your computer problems get fixed FAST. And since most repairs can be done remotely using our secure management tools, you don't have to wait around for a technician to show up.

3. **100% No-Small-Print Satisfaction Guarantee.** Quite simply, if you are not happy with our work, we'll do whatever it takes to make it right to YOUR standards without charging you for it. And if we can't make it right, the service is free.

4. **12 Month Money Back Guarantee.** At 2Secure Corp, our goal is to safeguard your data and forge long-lasting relationships with our clients. That's why we stand behind our 100% satisfaction guarantee: If you are not satisfied with our services you will be completely refunded.

5. **Accurate Billing – Guaranteed.** Every bill you receive from us is guaranteed to be accurate and detailed. You'll know exactly what you are paying for, and ALL charges will be pre-approved by you. No more one-line "mystery" bills that don't outline what you are paying for.

6. **Experience.** With 24 years of extensive experience, we continue helping our clients feel secure yet running safely their business.

7. **Solutions.** Our client-targeted solutions are based on the latest and most current technological knowledge. We specialize in studying and understanding the client's needs and tailoring the ideal solution based on state-of-the-art technology.

8. **Peace Of Mind.** Because we monitor all of our clients' networks 24/7/365, you never have to worry that a virus has spread, a hacker has broken in or a backup has failed to perform. We watch over your entire network, taking the management and hassle of maintaining it off your hands. This frees you to focus on your customers and running your business, not on your IT systems, security and backups.

A Letter From The Author:
Why We Created This Report And Who Should Read It

From The Desk of: Yigal Behar
CEO, 2Secure Corp

Dear Colleague,

When you decided to look into transitioning your computer network and operations to the cloud, you were probably met with conflicting advice, confusion and no real answers to your questions and concerns over security, cost and whether or not it's appropriate for your organization.

That's why we wrote this report. **We wanted to give CEOs and business leaders a simple, straightforward guide that not only answers your questions in plain English, but also provides vital experience-based information that most IT companies don't know (or may not tell you) that could turn your migration into a big, cash-draining nightmare.**

My name is Yigal Behar My organization has been working for the past 13 years in Cybersecurity. The cloud revolution has brought many good improvements to business around the world. This change has a great privacy and safety impact. As it turns out, using cloud solutions will increase costs when a Security breach has been identified.

The simple fact is, cloud computing is NOT a good fit for every company, and if you don't get all the facts or fully understand the pros and cons, you can end up making some VERY poor and expensive decisions that you'll deeply regret later. The information in this report will arm you with the critical facts you need to avoid expensive, time-consuming mistakes.

Of course, we are always available as a resource for a second opinion or quick question, so please feel free to contact my office direct if we can clarify any points made in this report or answer any questions you have.

Dedicated to serving you,

Yigal Behar – CEO

2Secure Corp

Cloud Security Special Report

If you've been undecided about the move to cloud-based computing, you aren't alone, since only about 37% of all companies are currently adapted for cloud computing. However, a recent report issued by Emergent Research and Intuit Inc. projects that by the year 2020, approximately 80% of all US businesses will have fully embraced cloud computing, and will conduct their businesses in that mode.

Without you realizing it, your company may already be using cloud-based applications in various business units within your organization. For instance, if your company uses Dropbox as a means of exchanging documents or sharing them, you've already been using cloud-based applications.

Not surprisingly, these and a myriad of other web-based programs are enormously popular because of some of the inherent advantages that cloud-based computing imparts to them, namely tremendous flexibility, built-in automation, economy of scale, and universality of access via smartphones, tablets, laptops, notebooks, and even more devices which weren't even in the picture only a few years ago.

These reasons provide compelling justification for the dramatic shift toward cloud computing – its flexible delivery model alone has the capability to completely remake your business into a more dynamic and profitable enterprise, perhaps even saving you money in the process. More than any other improvable aspect of your business, cloud computing has the power to transform your company by delivering state-of-the-art applications, engaging users more fully and enhancing the online experience, and by making optimum use of the most modern online devices.

This collection of attributes has the potential to completely level the playing field for your company, allowing you to compete against much larger corporations by achieving an optimal online presence, and establishing your brand on an equal footing with the giants of your particular industry.

In this Special Report, we'll look at what you need to know about cloud security and computing, if you haven't already made the leap of faith it requires, and we'll survey the security aspects of cloud computing, so you can understand how the risks might be different from your in-house computing. Finally, we'll consider how you can secure your company's most valuable data assets while using the cloud, thereby gaining all the benefits while minimizing risks involved.

What Is Cloud Computing?

Wikipedia defines cloud computing as "the use and access of multiple server-based computational resources via a digital network (WAN, Internet connection using the World Wide Web, etc.)."

But what the heck does *that* mean?

The easiest way to not only understand what cloud computing is but also gain insight into why it's gaining in popularity is to compare it to the evolution of public utilities. For example, let's look at the evolution of electricity.

Back in the industrial age, factories had to produce their own power in order to run machines that produced the hard goods they manufactured. Be it textiles or railroad spikes, using machines gave these companies enormous competitive advantages by producing more goods with fewer workers and in less time. For many years, the production of power was every bit as important to their company's success as the skill of their workers and quality of their products.

Unfortunately, this put factories into TWO businesses: the business of producing their goods and the business of producing power. Then the concept of delivering power (electricity) as a utility was introduced by Thomas Edison when he developed a commercial-grade replacement for gas lighting and heating using centrally generated and distributed electricity. From there, as they say, the rest was history.

The concept of electric current being generated in central power plants and delivered to factories as a utility caught on fast. This meant manufacturers no longer had to be in the business of producing their own power with enormous and expensive water wheels. **In fact, in a very short period of time, it became a competitive necessity for factories to take advantage of the lower-cost option being offered by public utilities.** Almost overnight, thousands of steam engines and electric generators were rendered obsolete and left to rust next to the factories they used to power.

What made this possible was a series of inventions and scientific breakthroughs – but what drove the demand was pure economics. Utility companies were able to leverage economies of scale that single manufacturing plants simply couldn't match in output or in price. In fact, the price of power dropped so significantly that it quickly became affordable for not only factories but every single household in the country.

Today, we are in a similar transformation following a similar course. The only difference is that instead of cheap and plentiful electricity, advancements in technology and Internet connectivity are driving down the costs of computing power. With cloud computing, businesses can pay for "computing power" like a utility without having the exorbitant costs of installing, hosting and supporting it on premise.

In fact, you are probably already experiencing the benefits of cloud computing in some way but hadn't realized it. Below are a number of cloud computing applications, also called SaaS or "software as a service," you might be using:

- Gmail, Hotmail or other free e-mail accounts
- Facebook

- NetSuite, Salesforce
- Constant Contact, Exact Target, AWeber or other e-mail broadcasting services
- Zoomerang, SurveyMonkey and other survey tools
- LinkedIn
- Twitter
- All things Google (search, AdWords, maps, etc.)
- DropBox
- Microsoft AZURE
- Amazon AWS

If you think about it, almost every single application you use today can be (or already is) being put "in the cloud" where you can access it and pay for it via your browser for a monthly fee or utility pricing. You don't purchase and install software but instead access it via an Internet browser.

What About Office 365 And Google Apps?

Office 365 and Google Apps are perfect examples of the cloud computing trend; for an inexpensive monthly fee, you can get full access and use of Office applications that used to cost a few hundred dollars to purchase. And, since these apps are being powered by the cloud provider, you don't need an expensive desktop with lots of power to use them – just a simple Internet connection will do on a laptop, desktop or tablet.

Different Types Of Cloud Solutions Explained:

Pure Cloud: This is where all your applications and data are put on the other side of the firewall (in the cloud) and accessed through various devices (laptops, desktops, iPads, phones) via the Internet.

Hybrid Cloud: Although "pure" cloud computing has valid applications, for many it's downright scary. And in some cases it is NOT the smartest move, due to compliance issues, security restrictions, speed and performance. A hybrid cloud enables you to put certain pieces of existing IT infrastructure (say, storage and e-mail) in the cloud, and the remainder of the IT infrastructure stays on-premises. This gives you the ability to enjoy the cost savings and benefits of cloud computing where it makes the most sense without risking your entire environment.

Single Point Solutions: Another option would be to simply put certain applications, like SharePoint or Microsoft Exchange, in the cloud while keeping everything else on-site. Since e-mail is usually a critical application that everyone needs and wants access to on the road and on various devices (iPad, smartphone, etc.), often this is a great way to get advanced features of Microsoft Exchange without the cost of installing and supporting your own in-house Exchange server.

Public Cloud Vs. Private Cloud: A public cloud is a service that anyone can tap into with a network connection and a credit card. They are shared infrastructures that allow you to pay-as-you-go and are managed through a self-service web portal. Private clouds are essentially self-built infrastructures that mimic public cloud services, but are on-premises. Private clouds are often the choice of companies who want the benefits of cloud computing, but don't want their data held in a public environment.

Cloud Computing - What You Should Know

The first thing to know about cloud computing is that it has now become the overwhelming champion of strategic technology around the globe, and is estimated to approach $200 billion in value as an industry by the year 2020. This isn't just an accident of course – the cloud computing market has been dramatically powered like this by the business need for flexibility, speed, and universal access from any location, by any device. Because the cloud has so much to offer, its appeal has already soared to the forefront as a transformer of businesses.

But that's just the beginning. Having already delivered the tools to help drive complete business transformation, the cloud is now quickly becoming the enabler for process improvement, as well as for providing an enhanced and more engaged customer experience. As if there were any doubt, a survey recently conducted by KMPG documented that close to 1,000 leaders in the technology industry consider cloud computing to be the single most pervasive technology in changing the way companies do business over the next several years.

Cloud computing has the capability to affect almost everything about the way you do business, and to improve on what you've been doing by providing efficiency gains and more creative approaches. The KMPG survey emphasized that some of the business areas currently being altered dramatically by cloud technology are data analytics, total cost of ownership, greater alignment between customers and business personnel, empowerment of the mobile workforce, faster time to market, and a pronounced movement toward global business models.

Here's a key thing to understand about cloud computing – it isn't simply a platform which will allow you to do what you're doing in a better way (although it does that), but it is poised to become the foundation upon which future innovation will be built for some time to come. It's not just about cost savings and efficiencies, it is an enabler for the most advanced new technologies on the horizon, and if your company can embrace these new technologies and make them part of your business, it will go a long way toward keeping your business competitive, and possibly gaining a step on your rivals.

What About Security On The Cloud?

Right from the beginning, security has been a kind of fly in the ointment for cloud computing, and the one objection most commonly tendered by businessmen considering a move toward the cloud. As opposed to the supposed safety of keeping valuable data assets in-house and under the protection of motivated company employees, it seemed like inviting vulnerability to have critical business information be re-positioned on servers somewhere else, under the care and management of people who had no personal interest in its safety.

Are there risks associated with migration to the cloud? Absolutely. However, from the above it should be apparent that the enormous advantages offered by cloud computing far outweigh any risks involved in moving to that platform. The truth is, your business data is no safer in-house than it would be on the cloud, and no more at risk. Cyber criminals are out there, and they'll find you and your business whether

you're on the cloud, or whether you've battened down the hatches of your own standalone computing environment, thinking about how safe and secure your business is. If you're connected to the Internet, you're at risk.

The Four Major Assailants Of Your Network

It should be borne in mind that these four categories of data asset attackers do not operate solely against cloud-based businesses; as stated above, your business data is no safer from a determined cyber criminal within the walls of your own building than it would be on a server farm somewhere on the cloud. Attackers could care less about physical location – all locations represent a source of income to them.

That being said, here are the **four categories** of the greatest security threats in operation today: **cyber-crime**, **cyber espionage**, **hacktivism**, and internal **employees**. You may be a bit startled by that last category, so let's tackle it first. In a study published by the Wall Street Journal recently, it was announced that as many as 75% of all employees take advantage of the opportunity of stealing data from the company they still work for, or have recently left.
This can involve stealing lists of customers, research information from an R&D department, or even managers taking any kind of information with them which might help at a new job. Maybe you haven't thought of your own employees as a security threat before, but who has better opportunity than someone on the inside? Hackers spend all their time trying to penetrate security defenses and get inside – internal employees are already there.

Hacktivism may also be a bit of a surprise, and is perhaps a term you aren't really familiar with. This form of attack has come to light in recent attacks against SONY, which was apparently targeted for political reasons by a group sponsored by North Korea, in retaliation for a SONY movie portraying that country's leader in an unflattering light. Apparently bent on making a statement to the world, these hacktivists secured their desired headlines by hacking into the computer systems of those companies. This form of attack does not appear to be motivated by monetary gain, but simply to announce the power of the attacker, and to put a global spotlight on their political or social agenda.

Cybercrime by contrast, has been around for quite a while, and is still enormously popular because it is so difficult to prevent and because the rewards are so significant for attackers. Credit card theft comprises the majority of such attacks for obvious reasons, but there are also thefts of insurance data, email addresses, and medical records, which can be used to leverage financial gain for the cyber criminals.

Cyber espionage is often used by commercial rivals, or is a state-sponsored criminal activity which seeks to gain entrance to networks containing intelligence information, to be used for political advantage or to gain leverage with international dealings. China and Russia are major players in this arena, but they are by no means the only players.

How Cyber Criminals Breach Your Defenses

At the outset of this discussion, you should realize that the simple and somewhat disturbing truth is that security is not nearly so much a technical problem as it is a people problem. If employees were better trained with an understanding of how security really works, there would be far fewer breaches of networks, and cyber attackers would be a lot more frustrated than they currently are. As it is, cyber attackers are well aware of the fact that the weakest link in any network is almost always the people who

administer it and access it on a daily basis. Beside the human-based vulnerabilities, there are also some technically-oriented aspects of security threats:

- The latest and greatest malware – robotic malware currently rules the roost when it comes to compromising computer systems. 'Bots', as they are called, commonly get installed on your computer when you open infected attachments and emails or download infected files from websites
- Mobility trends – many employees don't think twice about storing company data on their smart phones or other mobile devices, creating a blurry line between work and personal lives. Potentially sensitive data can thus easily be stored and transmitted from mobile devices with no real thought about security
- Social media vulnerability – the use of social media has become so prevalent, even during work hours by employees, that many employees give no thought at all to revealing sensitive information about themselves or their company in chat sessions. Any number of attacks have been reported where men have freely given up company information – even including passwords – to especially friendly female chat partners, who turned out to be clever male hackers
- Cyber terrorism – highly capable hackers now have the ability to take down entire power grids, and hold other components of infrastructure hostage in order to achieve their objectives
- False sense of compliance security – many companies make legitimate efforts to become compliant with security standards, and once they achieve that, they simply stop working on security or worrying about it at all. In actuality, most compliance rules are only intended to set a company on the path toward security, but not to actually address the underlying issues with security. This explains why companies who may be in full compliance with security standards get hacked all the time
- Advanced persistent threats – also known as APT's, advanced persistent threats are network attacks in which an unauthorized person gains access to a network, and stays there undetected for a long period of time. The intention of an APT attack is to steal data rather than to cause immediate damage to the network or organization.
- Internal threats – with practically every successful cyber crime carried out, there is an internal breach at the bottom of it. This may be an intentional compromise such as accepting a bribe, or a completely unintentional weakness exposed by an employee through sheer ignorance.

Security on the cloud vs. in-house security

As previously mentioned, your business data is not entirely safe from attack no matter where it is physically located, so for the most part, there is no greater threat to your valuable information assets on the cloud than on your own premises. However, there are some issues specific to the cloud which should be considered, such as where it's actually stored, who has access to it, and what kind of regulatory measures govern maintenance of it.

Whereas on your premises, you have complete control over your data and all access to it, on the cloud you never really know where it's stored or who can access it. Because you never really know where your valuable information is being stored, there's no foolproof way to understand how it's actually being managed on your behalf. The nature of cloud services dictate that data is highly distributed and very much virtualized, so that your company's data could actually be physically located almost anywhere in the world, subject to those locations where your cloud provider has a physical presence.

Since your data would reside on the cloud, anyone who can access the cloud would theoretically have access to it, and it could also 'leak' into other companies' data simply by virtue of physical proximity. Granted, a cloud provider would take steps to minimize this risk in its management processes, but it is a risk nonetheless.

In addition, your company data could actually be located somewhere in the world which has relatively weak laws protecting the intellectual property rights of your data. This puts the onus on you and your company to have a thorough understanding of important contract points with your cloud provider, and to understand exactly where your data will be stored and who has access to it. The time to bring all this up is during negotiations with your provider, at which time you should insist on an arrangement that you feel comfortable with, and which will ensure the ongoing protection of your company's most valuable data assets. Something that might provide you with an increased comfort level would be to include a provision for allowing greater visibility, by having a third party audit your cloud provider periodically.

Another issue specific to the cloud platform is that of data availability, and by this we mean having round-the-clock daily access, with no downtime. Of course, downtime would be just as possible on your own premises if you had a sudden hardware or software failure, but in that situation you'd be in complete control of any recovery effort, which means presumably pulling out all stops to get back online quickly.

As a matter fact, you probably even have some kind of redundant network configuration for just such occasions, and at the very least, you should have backups from the prior business day. On the cloud platform, there are no guarantees to cover these situations, unless they are stipulated in the terms of a contract with your provider.

What happens if the Internet connection to your cloud provider goes down? This is another situation where it's really up to you to make sure the scenario is covered somehow by the terms of your agreement, and that a downed connection can be remedied either by a redundant line, or by a guarantee of recovery within an acceptable time frame. This will come with a trade-off though - you would almost certainly incur increased costs for the privilege of having a redundant line or recovery guarantee.

Migrating To The Cloud

By 2020, more than 80% of all businesses will be on the cloud, so if you're not there yet, chances are you will be within just a few years. If you haven't given it your full attention yet, now is as good a time as any - but don't just give it a cursory examination. Consider it within the framework of issues that are really critical to your business:

- Your company's most valuable data assets – conduct a thorough assessment of where your valuable company data currently resides, for instance on the network, on employee desktops and laptops, and possibly even on mobile devices. Do you have a policy in place for backing up all this critical information somehow, and are those backups immediately accessible when needed?
- Applications – identify the applications most critical to daily productivity by your employees, and determine what the impact would be if you lost access to these applications for any period of time
- Appeal of your data – consider who would benefit by having your company data, and the potential avenues they might use to get at it
- Preventing data breaches – along with the understanding of what the most likely paths are for breaching your system, and how such breaches might be prevented, you should think about the human vulnerabilities. Part of this is being honest about how well-trained your employees are at recognizing threats, and not falling into traps set by cyber attackers

The point of all this heavy duty thought is to get a feel for how much risk is associated with migration to the cloud for your company. Although the tremendous benefits of cloud-based computing have been prominently lauded earlier in this discussion, not all of them apply to every business, and it might very well be that the actual benefits your own company would derive are not all that significant.

If your company is not one which thrives on innovation, and doesn't use the most modern tools and technologies, the appeal of the cloud will probably be considerably less for you. In any case, weighing the benefits achievable to cloud-based computing against the potential risks you identify for your company, should provide you with a fairly clear answer as to whether or not migration to the cloud is in your company's best interests.

No matter what you do, security will still be an important part of your business, even if most of your data and most of the applications used by your company are situated on the cloud platform. You still have to maintain in-house security for local applications, and you still have employees who are vulnerable to clever cyber attackers.

Security is so interwoven throughout the fabric of modern computing, that there is no such thing as simply farming out your data, your applications, and all the security measures it takes to protect them. Wherever computing is done, good security practices such as regular user training and monitoring threat intelligence will be necessary.

Free Assessment Shows You How To Migrate To The Cloud And Avoid Overpaying For Your Next IT Project Or Upgrade

If you're like a number of CEOs we've helped, you've already been burned, disappointed and frustrated by the questionable advice and **complete lack of service** you've gotten from other IT companies. In fact, you might be so fed up and disgusted from being "sold" that you don't trust anyone. *I don't blame you.*

That's why I'd like to offer you a **FREE Cloud Readiness Assessment** to show you there IS a better way to upgrade your computer network AND to demonstrate how a truly competent IT consultant (not just a computer "mechanic") can guide your company to greater profits and efficiencies, help you be more strategic and give you the tools and systems to fuel growth.

At no cost or obligation, one of my lead consultants and I will come to your office and conduct a thorough review and inventory of your current computer network, backups and technologies to give you straightforward answers to the following:

✓ How using cloud technologies may be able to <u>eliminate the cost, complexity and problems</u> of managing your own in-house server while giving you <u>more freedom, lowered costs, tighter security and instant disaster recovery</u>. I say "may" because it might NOT be the best choice for you. I'll give you honest answers to your questions and detail – in plain English – the pros AND cons of moving your specific operations to the cloud.

- ✓ Are your IT systems <u>truly safe and secured</u> from hackers, viruses and rogue employees? (FACT: 99% of the computer networks we review are NOT, much to the surprise of the CEOs who are paying some other "so-called" expert to manage that aspect of their IT.)

- ✓ Are your backups configured properly to ensure that you could be back up and running again <u>fast</u> in a disaster? From our experience, most companies' backups are an epic waste of money and only deliver a false sense of security.

- ✓ If you are ALREADY using "cloud" technologies, are you adequately protecting your organization from the dozens of ways you and your organization can be harmed, sued or financially devastated due to security leaks, theft, data loss, hacks and violating ever-expanding data privacy laws?

Even if you decide not to move your network to the cloud or engage with us as a client, you'll find the information we share with you to be extremely valuable and eye-opening when you make future decisions about IT. After all, it NEVER hurts to get a third-party "checkup" of your IT systems' security, backups and stability, as well as a competitive cost analysis.

There Is One Small "Catch"

Because our Cloud Readiness Assessments take between five and seven hours to complete (with most of this "behind-the-scenes" diagnostics and research we conduct), I can only extend this offer to the first seven people who respond. After that, we'll have to withdraw this offer or ask that you pay our customary consulting fee of $350 for this Assessment (sorry, no exceptions).

To respond, please call our office at 646-755-3933 and ask for me, Yigal. I personally want to take your call to answer any questions about this letter, my company and how we might be able to help you, CEO to CEO. You can also e-mail me direct at Yigal@2Secure.biz

Awaiting your response,

Yigal Behar
www.2Secure.biz
Call us direct: 646-755-3933