Seven Big Trends for Small Businesses in 2013

Today, if you tell someone you’ll be in touch, he or she now expect you not only to ask when, but how. Modern technology has dramatically changed the way we communicate, providing multiple ways to stay connected at any time. For small and medium-sized businesses, this means big opportunities to stay competitive, provided that they understand technology trends and use them to their advantage.

Check out these leading trends set to amplify in 2013, providing businesses with key ways to keep profits and customer satisfaction up:

**Trend 1: Look to the Clouds**
Everyone is talking about cloud technology these days, which basically means remote computing, leveraging the Internet. This is great news for small and medium-sized businesses because cloud-based systems provide a plethora of tools, save costs and minimize maintenance. For example, cloud programs can help manage payroll, invoicing, phone systems, documents, customer management, business analytics and backup systems. Online cloud services commonly used by small businesses include Skype, Dropbox and Google Docs.

**Trend 2: The Era of Social Media**
Social media’s growth continues to boom, and businesses no longer have the option of ignoring this outreach potential. It’s cost effective and connects you to customers in ways never before possible. Use Youtube, Twitter, Facebook and blogs as part of your business’ social media program. The relationships you can build with key customers and the feedback they provide is invaluable.

**Trend 3: Your Workplace is Everywhere**
Technology enables people to stay connected and work from virtually anywhere, meaning the terms “off the clock” or “away from the office” are going extinct. Whether you’re working from home, at the office, or in a coffee shop, it is vital to be accessible at all times, especially if you run a small or medium-size business. Whether your preferred device is a laptop, tablet, or smartphone, staying connected is a must.

**Trend 4: Video Conferencing Instead of Business Travel**
Traveling is costly and time-consuming. Video conferencing is a low-cost way to meet with customers, prospects and suppliers from virtually anywhere with computer and Internet access. Common video conferencing resources include Skype, ooVoo and Cisco WebEx, making it easy to communicate with individuals or groups.

**Trend 5: Applications Keep Things Moving**
Apps are not just fun and games - many are made specifically for the mobile office, making on-the-go work easy. Plantronics Instant Meeting app, for example, allows one-click access to conference calls from a smartphone - no need to remember long conference codes and leader PINs when you’re out and about. Other useful mobile office apps include Documents to Go and QuickOffice, providing efficient access to documents, agendas and analytics.

**Trend 6: Talk Just Got Cheaper**
Long distance phone calls to employees, customers and prospects can quickly increase a phone bill. Internet-hosted phone systems are becoming more popular because they are low cost, flexible and low maintenance. Skype is a good example of a voice-over-Internet service that allows individuals to communicate through video, voice and instant messaging using a headset.

**Trend 7: Devices Talk Amongst Themselves**
Think how much more effective your communications would be if all your devices worked together. Fortunately, that now is happening and the technology trend is aptly called Unified Communications (UC). It delivers voice, email, SMS, video conferencing and document sharing into a single interface so that you can easily relay any or all of your data to others.

With a laptop, Internet connection, Skype and a headset, you can conduct business from just about anywhere at any time. To learn more about these trends, visit www.plantronics.com/BigTrends. Even though at first it may seem overwhelming to adopt each of these trends, when you do, you’ll find that it’s easier than you think and a smart way to help your business thrive.

ARA Content
YOUR ENDPOINT SECURITY SOLUTION

A pioneer of the antivirus industry
ESET created one of the first antivirus solutions in the world, and holds the world record of consecutive VB100 awards.

ESET keeps your systems running 24/7/365
• Powerful, accurate detection
• Low false positives
• Data access and control

For more information or to request a free trial, visit us at www.eset.com
This is the first issue in an insightful new series from the San Diego Business Journal that features advice and commentary from regional experts on various aspects of technology and its applications in our new digitally-driven business world. Our first section focuses on evolving approaches to data management and storage from the “cloud” to traditional legacy systems. Future issues will feature tech’s influence on the business of health care, real estate, banking and finance.

Q: As businesses move more and more processes and transactions online, IT has taken a central role in some of the most important business-ethical issues of the day – privacy and the ownership of personal data. Changes in technology and business procedures can outpace a company’s ability to train employees to deal with these issues. What should businesses do to establish ethical parameters for managing data?

A: To ensure the safe and ethical handling of data, companies first need a clear and well-documented understanding of exactly what personal data they handle. Depending on the type of business, a company’s systems may contain personally identifiable information (PII), relating to its customers or employees or both. You need to know where PII in your systems comes from, where it is stored, where it goes, and who needs to access it. You should also know what legal requirements pertain to the information (as these may not align exactly with ethical constraints on the use of PII).

Now you can make informed decisions about what information to protect and what form of protection is appropriate. Typically this means restricting PII access to only those employees who have a need to see it. Using technologies such as encryption and scanning, authentication requirements including firewalling, intrusion prevention measures, malware scanning, authentication requirements (should be multi-factor), redundancy, backup, and site security.

Q: What security issues might my business need to address in planning to migrate our business to the cloud?

A: Turning to the cloud for IT services can be economically appealing but definitely involves a variety of risks that vary according to the type of cloud. If you use a public cloud approach then some or all of your company data and applications will be in a shared environment, potentially at risk from bad guys attacking that cloud or from the actions of others sharing that environment. You also face potential risks from the actions of the cloud provider itself such as failing to provide sufficient redundancy to cope with weather related outages.

Public cloud providers do make security assurances but those are unlikely to be backed by a Service Level Agreement (SLA). A set of tests run by RAE Systems last year found that several public clouds failed to notice malicious traffic, whether it was inbound or outbound. A private cloud removes some of the concerns of a public cloud but you still need to perform due diligence, asking prospective providers about their security measures, including firewalling, intrusion prevention measures, malware scanning, authentication requirements (should be multi-factor), redundancy, backup, and site security.

Q: Technological change can be very expensive for an organization involving purchase and installation of equipment, maintenance, training and replacement/upgrading. What advice would you give to companies looking to evolve to a more technologically-driven business operation, but are resistant because of potentially high costs?

A: One of the biggest questions facing decision-makers today is whether to invest in IT infrastructure or start migrating to cloud services. But let’s face it: there is little need to build and operate your own IT gear when such services can be sourced much more affordably and flexibly via the cloud.

When doing the math of “build vs. buy”, it is easy to overlook factors not directly associated with initial purchase, such as the value of all the time required to source, configure, implement, monitor, upgrade, and troubleshoot equipment; annual hardware and software maintenance fees; ability to ramp resources up and down easily when demand changes; and the need to hire, motivate, and retain dependable IT talent.

Bottom line – the operational and financial reasons for migrating to cloud services are quite compelling. In other words, can you afford NOT to do it? Don’t simply fall prey to the old way.

Q: With Moore’s Law and the rapid rate of change in computer technology, it seems that commoditization is rampant and business advantage quickly moves to the largest players with the greatest economies of scale – think Amazon, Cisco, Google, Microsoft, and more. What advice can you give to businesses that want to harness this power for greatest value?

A: Frankly the risks for security breach or data leakage with cloud services are no different than for legacy-sourced services. There are not inherent advantages or limitations due to technology; it basically comes down to access policies, data segmentation, training, trust, and oversight. Indeed, screen captures, copied files, and memory sticks take mere seconds regardless of a person’s actual location; people are still the source of most vulnerability, not the technology.

In fact, from an IT security standpoint, the level of privacy, isolation, and verification on enterprise-class cloud services are often higher than what is found with legacy implementations. Why? Specialization and investment. Because cloud service providers do it for hundreds of clients every month who expect a very high level of assurance, such providers have invested in and “over-engineered” services and procedures to satisfy even the most stringent customers.

Continued on Page S26

Continued on Page S26
From **cloud**, **security**, and **network services** to **disaster recovery** and **colocation**, AIS provides reliable, secure, enterprise-class data center solutions in **San Diego** and **Phoenix**.

**SERVICE**
Why Do IT In-House? From cloud, security, and network services to disaster recovery, colocation, and managed services, AIS makes it easy for clients to get what they need.

**EXPERTISE**
People Matter. With over 150 years of cumulative IT services experience across the senior leadership team, AIS knows what it takes to deliver superior client satisfaction.

**SUPPORT**
Compliance Counts. AIS upholds the highest levels of SSAE 16 compliance and ITIL v3 service management in each of our SOC 1, 2, and 3-audited data centers.

**MEET WITH US AT THIS EVENT ON WEDNESDAY, MARCH 6**

“Migrating to the Cloud”
Featuring Dr. Timothy Chou, Stanford University
And CIOs from Amylin, Qualcomm, SDG&E
Wednesday, March 6 from 5:00 to 7:45 pm

Qualcomm Headquarters, Building N
Irwin M. Jacobs Qualcomm Hall
5775 Morehouse Drive
San Diego, CA 92121

www.americanis.net  866.971.2656 phone  sales@americanis.net
Employees are going to download files in their day to day activities of their jobs. How can I ensure that I’m not putting our business’s core data at risk with hidden virus and malware running rampant these days?

A well-designed IT system will provide multiple layers of defense against malicious and unwanted file downloads. You can configure systems to prevent unauthorized downloads, either by type of file or source of file (for example, blocking downloading of unauthorized executable files and blocking surfing to adult sites). You can install antivirus scanning at the file server and email server level, right down to the individual computers or endpoints, including smartphones and tablets. A good antivirus program, properly installed and well-maintained, will block the vast majority of malicious code that is out there in the wild, from viruses and worms to Trojans and time-wasting nuisance apps (sometimes referred to politely as potentially unwanted applications).

Of course, the most critical layer of defense is the human layer. You need your employees to know why they should abide by IT security policies and refrain from downloading unauthorized files. A workforce that understands the risks that such files pose to the well-being of the company, as well as their hopes of continued employment, is less likely to ignore warnings, override settings, or try to defeat your layers of defensive technology.

We welcome your feedback and comments: BJ Ghiglione 858.277.6594, bghiglione@sdbj.com