

BUSINESS

ONLINE FROM WALL STREET TO MAIN STREET, KEEP UP WITH THE LATEST ECONOMIC HEADLINES

Business

909-483-9391

Business Reporter Andrew Edwards 909-483-8550

GOT NEWS? WE WANT IT

Email your economy-related news items to us at bizz@inlandnewspapers.com or call 909-483-9391.



MIKE STULL

Cash flow, the oxygen of business

Take a deep breath. Now hold that breath for as long as you can.

The record for breath-holding on land is around 10 minutes. If you are like most people, you cannot even get near that time. Nor would you want to — the intake of oxygen is critical to continue living.

In the business world, the equivalent of oxygen is cash. Without cash, a business does not survive. Cash flow — the constant inflow and outgo of cash in a business operation — is literally the lifeblood of a business. It also one of the biggest challenges entrepreneurs and small-business owners face.

You might be thinking that this is pretty obvious — if a business is not earning money, it clearly will go out of business. This is not what I mean. Let's assume that a business is enjoying a healthy sales level — it can still have a shortage of cash — "negative" cash flow.

When more money is going out than

Q AND A: MARTY KAUFMAN Founder, Accent Computer Solutions

Who's minding your store — of data?

By Andrew Edwards
Staff Writer

RANCHO CUCA-MONGA — Any business owner who uses computers needs to be mindful that some criminal or disgruntled employee may one day find a way to hack in and steal data or cause any number of problems, says the founder of an inland information technology firm.

Accent Computer Solutions is a business that provides information technology consulting, tech support and computer security services to other businesses.

"We're an outsourced I.T. department for companies to 15 to 500 desktops so we have to be good at everything," founder Marty Kaufman said.

Accent, which has 32 employees, has been in business since 1987. The company has always been headquartered in Rancho Cucamonga and has branch offices in San Bernardino, Riverside and Los Angeles.

One customer, he said, contacted



KAUFMAN

Accent after a particularly scary security breach:

"I had a user where the FBI walked in the door and said you're an illegal porn site. And they didn't know. Everything has an IP address and it can be traced," Kaufman said.

"They obviously exonerated them and everything was fine, but they didn't know," Kaufman continued.

"We watch what nobody's watching."

Kaufman proposed that situation would have never happened if Accent had been on hand beforehand as a watchdog.

One of the worst errors a business owner can make, he said, is to assume that hackers will ignore one's computer system.

"When it happens, it's big," Kaufman said.

Question: What is the most common computer security problem for small businesses?

Answer: One of the branches is what people see, and then what they don't see. Security is invisible

to the user unless something bad happens.

What we see is adware, or maybe malware. You click on something and something's flashing and now you're in trouble. ...

What you don't see is malicious code on the website ... where somebody's harvesting information on your website. Or unauthorized users on your wireless network. ...

The No. 1 security problem in all companies today is the inside disgruntled employee. Somebody has the keys to the castle.

Q: What's the best way to defend against that disgruntled employee?

A: The best way is not have that function, is not have that risk, that I.T. risk that's internal.

The way to do that if you have an I.T. manager is to outsource as many functions as possible. It's the same as in accounting, not having the same person who counts the money take the checks to the bank. You've heard of that problem haven't you? Those same principles aren't applied to I.T.

Q: What is the most frequent

mistake small-business owners make when setting up an I.T. system?

A: Let's go to security on that. Now were going to the area of what they should do, versus what they do. Let me give the very basics of doing it right. What they need is a managed firewall and what that means is they need somebody in charge go keeping it up to date.

No. 2 is they need some sort of web filter that controls what users are able to do on a day-to-day basis. ... A lot of times, my customers' computers aren't working because they (employees) are watching TV, or March Madness.

The next thing is Microsoft and antivirus patches, and that's on the desktop.

And the last thing is passwords, as much as it sounds stupid, complex passwords that you don't share are a lot more secure than simple passwords. And by complex, I mean letters and numbers, and if the letters have to be capital (case-sensitive), that makes it more secure by an order of magnitude.

andrew.edwards@inlandnewspapers.com
909-483-8550