Build a Winning Plan to Recover From Disaster Faster

By Judy Hector

It's tough to think about the many things that could destroy everything you've worked for. Besides being a gloomy topic, thinking about losing a key client, discovering that a trusted employee really isn't trustworthy, or even imaging your office getting flattened by a mudslide is the inverse of the way you naturally think. After all, working in the advertising industry, you're tuned into finding—and focusing on—the positive and the possible instead of pessimistic gloom-and-doom scenarios.

Reality is, horrible things can and do happen. And a lot of the time there's nothing you can do to stop it.

But what you can do, is develop a plan to mitigate the impact—and in some cases take preventative action—to protect your agency.

The first step is to figure out what threats are real, and how real they are. For example, if your shop is in San Francisco, you should be concerned about earthquakes but probably don't have to worry about tornados.

Continued on the next page

Continued from previous page

On the other hand, a Tulsa agency should flip that and plan for a tornado while keeping earthquake danger low on the list.

Other threats might be heavy snowfall, fire, theft, embezzlement, or losing a big client or key employee. Disengage your optimism and the myriad of potential disasters will be apparent.

You can't control Mother Nature

Even if your shop doesn't straddle a fault line or hunker down in Tornado Alley, you should still consider natural disaster.

The King Agency in Richmond, VA learned how fast things can change when a flood destroyed their office. "There was a foot of water on the floor when we left at 6:00 pm," says Dave King, the shop's president. "I have a clock on my wall, about six-and-a-half feet up, that was stopped at 6:25." With water rising faster than 13 feet per hour, there was little they could do. The next day, Dave was left with a bunch of month-old Macintosh doorstops and an 11-foot watermark on the wall. "Everything was ruined," he said.

"There was a foot of water on the floor when we left the office," Dave says. With water rising faster than 13 feet per hour, there was little they could do. The next day, Dave was left with a bunch of Macintosh doorstops.

"Everything was ruined," he said.

Luckily, their bookkeeper routinely made a weekly copy of the Clients & Profits database and took it off site.

"If I were to say that one thing saved the business," Dave says, "it was the fact that a copy of the C&P data was on a Zip disk outside the agency."

In the day-and-a-half that they were down, fellow agencies came to their aid, offering loaner computers and office space. "Everyone has been great," Dave says.

They forged ahead for 3 days, getting out whatever work they could until they could reinstall the C&P backup. "Work was tough for those few days without Clients & Profits," Dave says. "We didn't realize how much we need it."

When employees create havoc

Employees (either current or former) can also make a mess of things. From malicious treatment of files and equipment to inadvertent stupidity, your staff can do serious damage to your agency in seconds.

Did that cranky AE swipe a copy of your client list? Does that intern really know how to enter A/P invoices—or is she just faking it?

Don't forget about the technology junkie who stays late now and then; he could be using your shop's equipment for illegal activities. Or maybe he's just moving a few client files around—and accidentally deletes the final version. Whoops.

How do you keep these dangers at bay? Besides using old fashioned vigilance, use technology. Install computer monitoring software that tracks web sites visited, keystrokes, and other user information. (You might be surprised at what you learn.) Consider setting up timed lock-outs and passwords on terminals, and limit internet access. You can also use Clients & Profits access privileges.

Stopping sticky fingers

Embezzlement happens, and probably more often that you know (only about 120 in 500 business actually catch embezzlers). And, the Association of Certified Fraud Examiners says, an embezzling worker swipes about $127,000 before getting caught.

Continued on the back page

PLAN FOR THE WORST (and it won't be that bad)

Dotted your i's and crossed your t's? Completely convinced that everything is safe and secure when you're not looking? Look again.

Maybe you're safe from hurricanes, volcanoes, and earthquakes. But what about snow, fire, a wayward back hoe grinding your T1, or an office-wide outbreak of food poisoning?

The American Red Cross estimates that as many as 40% of small- to medium-sized businesses never reopen after a natural disaster hits. Why? Although they had insurance to replace physical assets, they didn't have adequate protection (i.e., off-site backups) for their digital assets.

Develop a plan now to ensure the continuity of your time-sensitive business functions, right down to who gets the mail. Build your plan with these 4 steps:

1. Take a look at potential threats, from that serene creek outside your window to the hot-headed spouse of the new AE, then determine the risk factor of each possible event.

2. Take steps now to minimize the loss if something happens. For example, if a key vendor is somewhere that disaster hits frequently, consider finding an alternate.

3. Decide now what to do if a disaster does strike so that the impact is minimized. Include an immediate workspace (your garage?), and be prepared to phone your employees, clients, vendors, and banks.

4. Set up a recovery plan. Include plans that will lessen the impact of long-term results, such as the logistics necessary for finding a short-term workspace, reinstalling data, and more.

Building a contingency plan is never fun, but you'll be back in business sooner than you think with an airtight plan (stored off site, of course!).

6 SYSTEM CONTROLS YOU CAN'T AFFORD TO OVERLOOK

By Chris Lawrence

Using firewalls is the first line of defense to keep your system safe from outside intruders. But what about insiders?

Nearly everyone is capable of wreaking havoc on your database and stored files. But your system manager can take simple (and often overlooked) steps to make sure that your shop's files stay safe from cranky employees and IT idiots.

First, make sure that everyone changes their passwords often, at least monthly. You can take this one step further and assign passwords to your staff instead of letting them choose to help prevent easily deciphered (i.e., hackable) user access.

Next, limit user access to the servers. Set them up in the system manager's office (no one will get past the system manager unscathed) or lock them in a room.

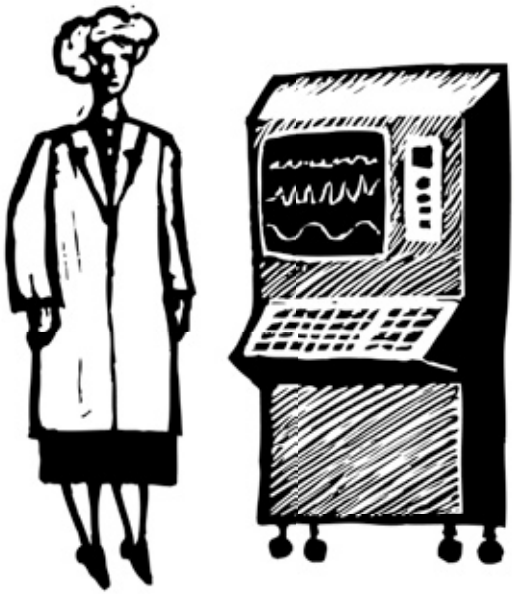
Control who has access to which files by segmenting your server or storing information in different places, such as putting your Clients & Profits database on a different server than your client files. Use server permissions to create custom access to servers, such as read-only or read/write, in addition to log-in privileges.

When someone leaves your company, be sure to deactivate them as a user in Clients & Profits, especially if they have remote access set up through My C&P! If they have other remote access to your servers, be sure to change their passwords or delete their access altogether.

And of course, when you and an employee part ways, change the alarm code and collect their keys.

Remember, your system can be the conduit for mayhem or the vehicle for security. But no matter what technical gizmo you've got installed, it won't stop bad guys from trying. But pair your technology with good old-fashioned vigilance and you'll have a pretty solid—and secure—system.

Chris Lawrence is a senior member of the Clients & Profits Helpdesk.



How to safeguard data from... Melvin

When thinking about safeguarding your data, you probably think about outside threats or disgruntled employees. But what about the good employee, hard working Melvin?

Melvin the...

... bad speller. He's writing an invoice note to a client to help them better understand what's being billed. But, honestly, Mel can't spell! Turn on his Clients & Profits spell checker. It's an automatic way to improve his spelling.

... messy time tracker. He confuses one task for another or adds ten hours instead of one. Require time approvals. Staffers add their time as usual, a manager reviews an unapproved time report, and catches any errors. Once edited, time can be approved.

... accounting illiterate. He's daydreaming about winning the lottery while adding A/P invoices and edits account numbers to match his ticket. Safeguard against posting to a wrong G/L account by adding default G/L accounts and not letting users edit account numbers.

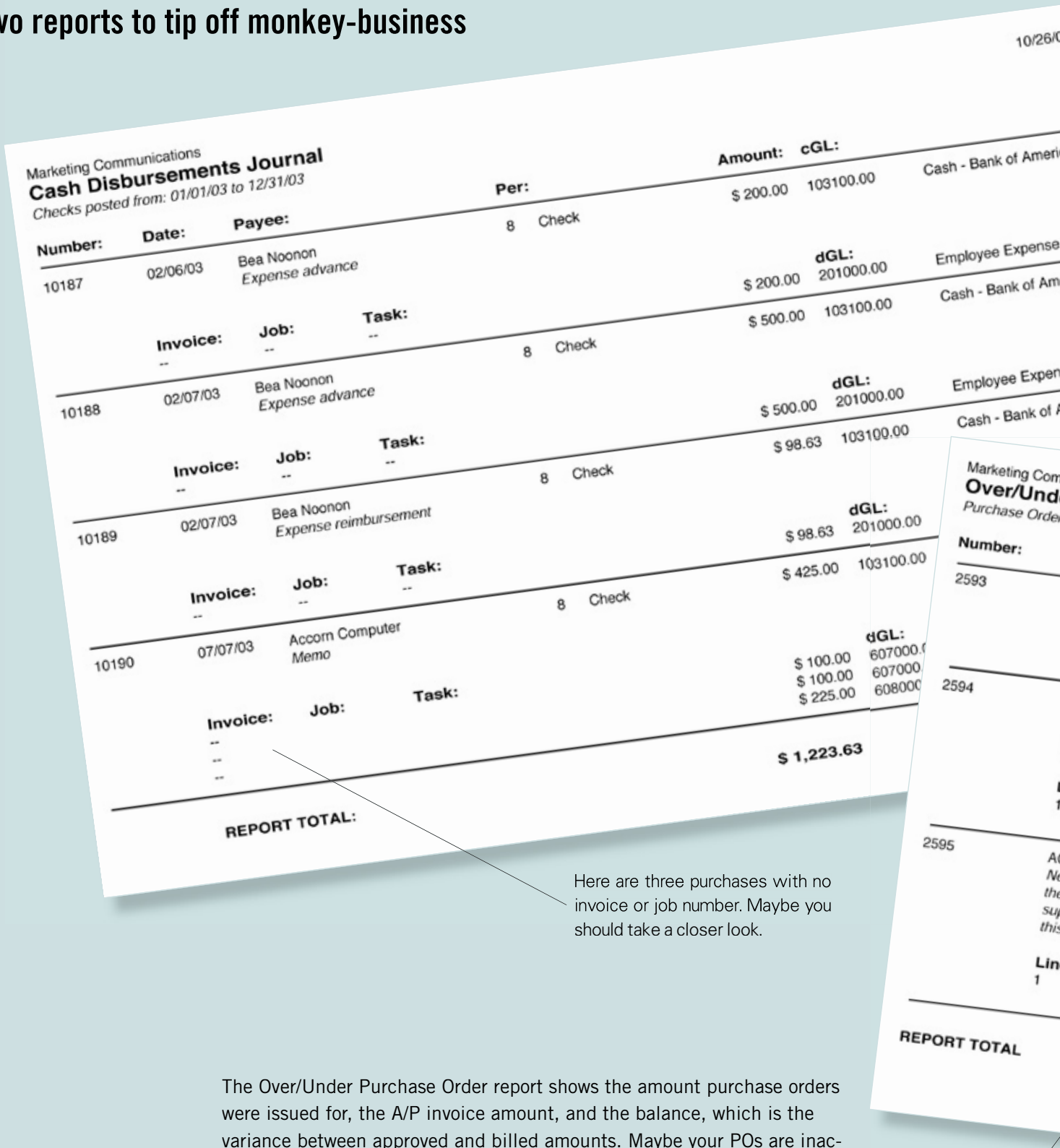
... crazy account coordinator. He's working for many AEs and isn't really crazy, just busy. Help him make adding new jobs quick, easy, and consistent. Use job type/spec sheets with the right tasks for work your shop does regularly.

... speeding traffic manager. Just get out of his way. Status codes classify a job's development but where's the safety net? Set up default status codes for new, closed, and reopened jobs so that no job is ever without one.

... world-class shopper. His dream job is being a buyer for HSN; but right now, he's working for you. Can't control his usual impulse to buy the biggest, baddest, and best? Set a dollar amount limit to purchase orders that he adds to control his purchases even when you're not around.

KNOW WHERE THE CASH GOES

Two reports to tip off monkey-business



Marketing Communications
Cash Disbursements Journal
Checks posted from: 01/01/03 to 12/31/03

Number:	Date:	Payee:	Per:		Amount:	cGL:	
10187	02/06/03	Bea Noonon *Expense advance*	8	Check	$ 200.00	103100.00	Cash - Bank of Ameri
					$ 200.00	dGL: 201000.00	Employee Expense
	Invoice: --	Job: --	Task: --				
10188	02/07/03	Bea Noonon *Expense advance*	8	Check	$ 500.00	103100.00	Cash - Bank of Am
					$ 500.00	dGL: 201000.00	Employee Expen
	Invoice: --	Job: --	Task: --				
10189	02/07/03	Bea Noonon *Expense reimbursement*	8	Check	$ 98.63	103100.00	Cash - Bank of A
					$ 98.63	dGL: 201000.00	
	Invoice: --	Job: --	Task: --				
10190	07/07/03	Accorn Computer *Memo*	8	Check	$ 425.00	103100.00	
					$ 100.00	dGL: 607000.(	
					$ 100.00	607000	
					$ 225.00	608000	
	Invoice: -- -- --	Job:	Task:				
REPORT TOTAL:					$ 1,223.63		

Marketing Com
Over/Und
Purchase Orde

Number:
2593
2594
2595

REPORT TOTAL

Here are three purchases with no invoice or job number. Maybe you should take a closer look.

The Over/Under Purchase Order report shows the amount purchase orders were issued for, the A/P invoice amount, and the balance, which is the variance between approved and billed amounts. Maybe your POs are inaccurate, maybe your vendor is greedy, or maybe it means there's something going on that you need to know about.

Do the amounts look right? Did the job really need 3 sets of film? Check this job ticket to be sure.

The Cash Disbursements Journal shows where your cash is going. Take a look at this report regularly to find any questionable payments (too frequent, odd amounts, unknown vendors, etc.). If you find something out of the ordinary, track the cost back to the physical invoice or paper receipt. It's better to be a little suspicious than a little (or a lot) ripped off.

Three expense advances in two days? What's that about?

This order is very old and hasn't been used t reconcile. Perhaps an A/P invoice was added—or not. Do the research.

This shows a $70 variance—the A/R invoice was posted for $70 more than the PO was issued for. Hmm....

04 14:47, Page 1

ca

Advance

erica

se Advance

America

munications

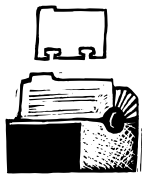
er Purchase Order

rs dated from 06/01/04 to 10/26/04

10/26/04, Page 1

Vendor:		Date:	Due date:	Status:	Net Cost:	Gross:	Balance:
B	B Printing	06/14/04	06/15/04				
Line: 1	**Job:** ABI-156	**Task:** PRNT	Printing				
ABG	AC Graphics	10/26/04			$ 25,000.00	$ 28,750.00	$ 25,000.00
1 - 8" x 10" 4/C film + Matchprint @ $125.00					**$ 25,000.00**	**$ 28,750.00**	**$ 25,000.00**
1 - 10" x 12" 4/C film + Matchprint @ $175.00							
1 - 12" x 14" 4/C film + Matchprint @ $215.00							
Line:	**Job:** 02-ABT-018	**Task:** FLM	Lithographic Film/Pre-Press				
G	Applied Graphics	10/26/04			$ 515.00	$ 605.90	$-110.00
eed a stat of the mechanical art. Please reduce so that					**$ 515.00**	**$ 605.90**	**$-110.00**
e largest dimension does not exceed 24". Please							
pply the percentage reduction of the stat to achieve							
s size.							
e:	**Job:** 02-ABT-019	**Task:** FLM	Lithographic Film/Pre-Press				
					$ 180.00	$ 211.77	$-70.00
					$ 180.00	**$ 211.77**	**$-70.00**
					$ 25,695.00	**$ 29,567.67**	**$ 24,820.00**

SECURITY QUESTIONS AND ANSWERS



Q. Since My C&P! isn't SSL, what is the best way to secure it?

The best way to secure My C&P! is by using a virtual private network. VPNs are a connection between two compatible firewalls over the internet. At one end, data is encrypted, then sent to the other firewall, which decrypts it using the same encryption key. By encrypting data before it's transmitted, external intruders are unable to use a packet sniffer to read the data during transmission. VPNs are a low-cost way to use the internet to keep sensitive information secure during transmission--and it costs significantly less than traditional dedicated connections.

Q. If someone uses my computer, will they have access to everything I have access to in My C&P!?

They'd have access if you don't quit your web browser and clear your cookies when you are going to be away from your desk for any period of time (like lunch or a meeting). The cookies for My C&P! do automatically expire after 8 hours.

Q. Where can I find news on current security issues?

On the C&P web site, read the Internet Access Security tech note: http://www.clientsandprofits.com/support/FAQs/tech_notes/technote_internet_security.html

There are many security related sites on the internet as well as trade magazines. One such example would be: http://www.securityfocus.com/

Q. How secure is a wireless network?

Wireless network security is really a matter of some debate. The security measures in most newer wireless routers provide a reasonable level of encryption. Yet, one has just to look at the number of wardriving and wireless hacking tools that are easily available to see that there is an active wireless hacking community. MAC address filtering (if your router supports it), and personal firewalls are highly recommended.

> Any time you are sending information over the internet, there is a possibility of someone being able to access it. There are always people out there who are going to able to beat your security. Keeping that in mind, there are some good security measures that you can use.

Q. What security concerns are there with remote access solutions?

Any time you are sending information over the internet, there is a possibility of someone being able to access it. There are always people out there who are going to able to beat your security. Keeping that in mind, there are some good security measures that you can use that will make it nearly impossible for someone to break. One such solution is PGP (Pretty Good Privacy), though this is used for file encryption (single file transfers) and e-mail: http://www.pgp.com/

As far as security with a multi-user relational database is concerned, the best lower cost solution is a VPN (Virtual Private Network). This can be used along with remote access solutions like Timbuktu or PC Anywhere (or similar 'remote control' programs) to provide a fast and secure connection. The absolute best solution is a point-to-point hardware-based encryption system, however this can be prohibitively expensive.

5 RED-FLAG REPORTS

Not every blip means trouble, but it could mean you should take a second look. There are dozens of reports in Clients & Profits that can help you spot trouble. Here are the Fab Five that watch commonly manipulated numbers.

■ **Clients P&L**. The Client P&L report shows each client's total billings and their budget, plus the variance. You'll also see a break out showing where the revenues came from and what the costs were. If anything is out of line, start snooping around.

■ **Vendor Account Ledger**. This report shows the payment amounts, dates, and check numbers for each vendor paid. Look for extravagant amounts, too-frequent payments, or unfamiliar vendors.

■ **Staff Realization**. Find out how many hours were worked and how many were billed. Off-the-chart numbers might mean fudged timecards or excessive client billings. Sub-par numbers might mean that someone is spending too much time doing things they shouldn't.

■ **Media Discrepancy**. The Media Discrepancy report can be run by either client or vendor. This report shows the net and gross media amounts ordered versus the actual amounts, as well as the A/P date. If the ordered and actual amount vary, find out why—and where the money went.

■ **Clearing Entries**. The Clearing Entries report shows the journal entries posted when account balances are transferred (or "cleared"). The report shows the date, period, accounts, and amounts. Sometimes transferring balances is appropriate, but too much transferring could spell trouble.

No report or software program can prevent someone from committing a crime. Remember, it only takes a few minutes to double-check something questionable, but it could take years to recover the loss.

STOP THIEVES IN THEIR TRACKS

By Judy Salkind

Here are the facts: Small businesses, especially those with fewer than 100 employees, are especially vulnerable to embezzlement. And it's usually an inside job.

Why? In small businesses, everyone wears more hats. With less segregation of duties, it's easier to hide the crime.

And, chances are, your agency feels a lot like family—full of people you like and trust.

Maybe there is no reason to suspect anyone (and you probably don't want to), but nothing is people-proof. Use these deterrences, because you'd hate to learn the hard way that you should have been suspicious.

■ Surprise! Do unscheduled cash audits to uncover any cooked books.

■ Have financial information mailed to your home instead of the office.

■ Make everyone take an annual vacation, and don't let their work sit until they return. When someone else picks up responsibilities, interesting things always turn up.

■ Separate financial responsibilities. The person who adds A/R shouldn't also add and sign checks or do the bank rec. Still another should pick up the mail. Better yet, have all of your financial statements mailed to the principal's home address.

■ Talk to clients and vendors to ensure that payments are being made. (Think of it as a schmooze opportunity.)

■ Scrutinize expense accounts and reimbursements. (One exec tried to deduct the same steak dinner three times. Busted!)

If you catch someone in the act, prosecute. It may be painful—especially if they were a trusted employee—but it sends a loud, clear message to everyone else.

It hurts to think that people you trust might try to take advantage of you. But it would hurt even more to lose a life's work to a greedy, soon-to-be ex-employee.

Judy Salkind is a senior member of the Clients & Profits Helpdesk.

THE BEST DEFENSE... IS A GOOD OFFENSE

Take a look at your security plan. Do you...

■ Use change orders to document what changes were made to a job, and why? When possible, have the client sign off on them to keep extra job costs in plain view.

■ Use the automatically-numbered POs in Clients & Profits? That way, every committed cost can be matched back to an invoice. Print a PO log to find any inconsistencies.

■ Always require that POs have an actual—and accurate—dollar amount? This will prevent sneaks from tacking on extra costs (and keep vendors from overcharging you, too).

■ Use prenumbered safety checks? Any out-of-sequence checks that show up on your bank rec are a big red flag.

■ Always have expense reports approved by a manager, and double-check expense amounts against receipts? Financial fraud includes dining on the company dime (when it's not company time), too!

■ Add clients payments and vendor invoices as they come in? This will minimize swings in A/P and A/R balances, making misappropriated financial transactions more apparent.

■ Spread financial responsibilities around? You're setting yourself up for a loss when only one person enters A/P, writes checks, and balances the accounts. Give many people limited access to financial responsibilities—and check up on the books yourself.

■ Talk to clients and vendors about recent jobs? It will be easier to verify billing and payment amounts if you have a good relationship with them.

SMARTER PLANNING (con't)

Continued from page 2

Embezzlement schemes to watch out for fall into four categories:

1) Billing - invoices for fictitious goods, inflated charges, or personal purchases;

2) Payroll - imaginary employees or unauthorized raises or bonuses are paid;

3) Expense reimbursements - phony or inflated expenses are turned in;

4) Check fraud - forged or altered checks are cashed, or checks are stolen.

And the cost of embezzlement goes beyond the loss of cash. Once the scheme is exposed, the trickle-down damage can cost top talent, clients, reputation, fiscal solvency, and company morale.

Who does it, and why

Unfortunately, the people most likely to hurt your business look like ideal employees. In a report that evaluated hundreds of cases over more than 10 years, 75% of the criminals were men, and most were first-timers with no criminal record. They were young, talented, and intellectual. By education, 42% were high school graduates; 45%, college graduates, and 13% had completed postgraduate work. But the common thread between all of them were motivation, opportunity, and the ability to rationalize their actions.

As a manager, you can't do much about what motivates employees to commit a crime. But you can interrupt opportunity and derail rationalization by creating a corporate culture that values ethical behavior and builds mutual respect. (For tips on spotting and stopping criminal behavior, see the article on page 7, "Stop Thieves In Their Tracks.")

Planning for the best

No matter how many precautions you take, bad things do happen. But if you plan to make the best of it when it inevitably happens, you'll be in the fast lane to recovery.

First, make a list of threats, rank them from most to least likely, then start building your recovery strategy. Include things like off-site back-ups, human resource policies, and, above all, vigilance.

Sounds like a lot of work? Truthfully, it is. But Clients & Profits can help, and you'll find tips throughout this newsletter. From access privileges to reports, there are dozens of helpful tools right at your fngertips.

It's easier to believe that you're immune from disaster (wouldn't that be nice?!). Unfortunately, the potential is as real as the paper you're holding. So, now that you're thinking about it, while everything is buttoned-up and secure, start planning. You'll never be sorry you did.

Judy Hector is Director of Marketing for Clients & Profits

CLIENTS & PROFITS®
The Triangle Building
4755 Oceanside Blvd. Suite 200
Oceanside, CA 92056
(760) 945-4334

www.clientsandprofits.com

Attn: CEO