focus

august/september 2013

Don’t be caught off guard

Employing cybersecurity for small businesses

Work with an expert when it’s time to value your company

6 ways to survive an IRS audit

Health care act may make HSAs more attractive

ZINNER & CO. LLP

29125 Chagrin Boulevard
Cleveland, OH 44122-4692
ph: 216.831.0733
fax: 216.765.7118
email: info@zinnerco.com
www.zinnerco.com

Don’t be caught off guard

Employing cybersecurity for small businesses

Large cases of cybersecurity breaches — such as the 2012 network infraction at online retailer Zappos that potentially exposed account information on more than 24 million customers — tend to dominate the headlines. But smaller businesses also are at risk. In fact, businesses with up to 100 employees made up nearly one-third of the organizations that had been victims of a breach in the preceding year, according to Verizon’s *2013 Data Breach Investigations Report*. As you can imagine, recovering from such an incident can be costly in terms of actual transgressions as well as damage to the business’s reputation.

So, how can you protect *your* company? Read on …

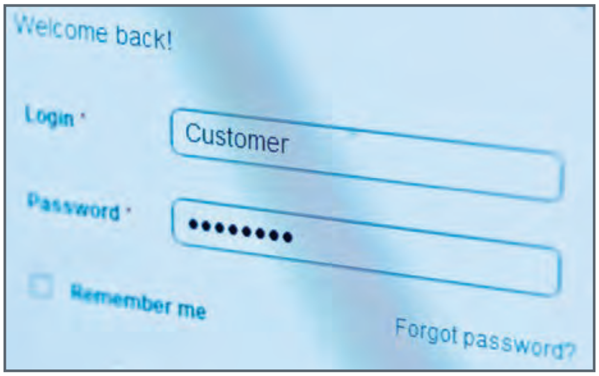
Addressing a serious threat

No matter its size, every business needs to take seriously the risk that its systems might be compromised, and act to reduce the likelihood of a data breach. Some 75% of the security breaks in the Verizon report were considered *opportunistic* attacks. That is, the perpetrators were able to penetrate an organization’s IT network with little difficulty.

No matter its size, every business needs to take seriously the risk that its systems might be compromised.

To avoid that outcome in your company, make sure you:

1. Develop a plan for managing data. Examine how and why you acquire, use and store data. What data do you need, and how can you obtain it with a minimum amount of risk?



How is it transmitted and stored? When can it be destroyed?

2. Classify your data. It’s impossible to protect every record, so focus on the information that’s truly sensitive. That requires knowing which records fall within this category. Customers’ financial information and patients’ health records are just a couple of examples of sensitive data.

3. Limit the collection of confidential data to just what’s necessary. For example, if your business doesn’t actually use customers’ driver’s license numbers, collecting them adds no value and exposes you to risk if a violation occurs. When you do acquire sensitive data, keep the number of devices on which it’s stored to a minimum, and limit access to only those employees who require it.

4. If you bank online, dedicate one computer to the task. Make Internet browsing, e-mailing or other cyber activities off limits from the computer. This cuts the risk that you’ll catch the attention of cyber criminals. Limit physical access to the computer to just those employees involved in banking functions.

5. Educate employees on cybersecurity policies. More than 75% of respondents to the report *The Human Factor in Data Protection* from the Ponemon Institute, a research firm, said they had experienced a data breach as a result of negligent or malicious employees or other insiders. To combat such behavior, show your employees how to develop a strong password and keep it private. They also should be instructed not to download attachments from unknown sources.

6. Use software tools to protect your network and data. Creating a firewall, for example, can prevent outsiders from gaining access to your network. Intrusion detection tools can monitor system activity, watching for attacks from both outsiders and from within. Also, harness an encryption program that converts data to a format that can't be easily deciphered by individuals who aren't supposed to see it.

7. Destroy data that's no longer needed and that you're not legally required to maintain. Even if the information no longer is useful, it still may contain sensitive information that can put your company at risk if an infraction occurs.

8. Clean computers that no longer are used. It's not enough to just delete the files, as the information may remain within the device. A more effective data destruction method is software that overwrites the existing information. Or you can physically destroy the device.

If your business engages an outside party to provide data security, request documentation explaining how the company protects your organization's information and systems. Also consider auditing the firm's data protection plans and systems.

Preparing for a break in security

No data protection plan can completely eliminate the risk of a breach. Even as you work to limit the likelihood that your records and systems will be compromised, you also want to outline the steps you'll take if a violation occurs.

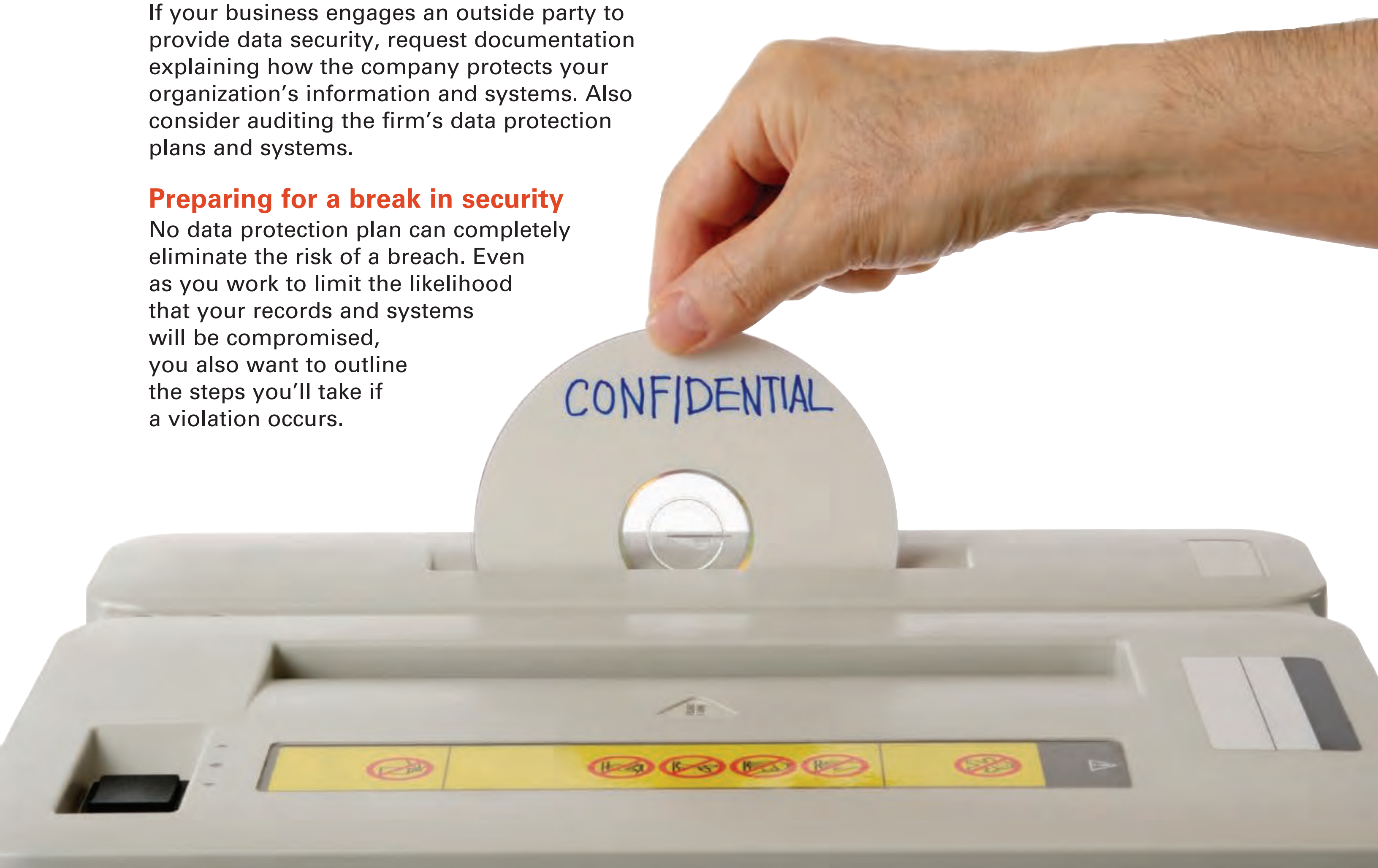
The first step is to create a team that will respond to the breach. While the makeup of that group will vary by company, typical members will include management, IT, legal, and your marketing or public relations group.

It's also critical that your company understand the laws that govern data violation notification in your industry and state. You may be required to notify customers of breaches that could compromise their personal information.

Of course, you should act quickly to contain any infraction. This may require powering off a server or going offline for a period of time. In such cases, take steps immediately to recover any information that's been lost. For instance, you may need to restore data from the most recent backup. To limit the negative impact of a break in security, call in your legal, computer, public relations or other outside experts.

Reducing your risk

Security breaches can be devastating to a business. However, you can reduce the risk by securing your networks and devices, properly training employees and managing the data they collect. ⟐



Work with an expert when it's time to value your company

Oftentimes, business owners require a valuation of their company. Some might believe that they know the value of their business down to the last penny. But they'd likely be wrong. Placing a correct value on a business is only achieved via a complicated process, which is best left to a professional appraiser.

The purpose behind a valuation

There are numerous reasons for performing a valuation. For example, you may want to buy or sell a business, set up a buy-sell agreement or target some strategic goals. There are other reasons as well: You may want a valuation to establish an employee stock ownership plan or to secure financing and credit.

Tell your valuator about rules of thumb and other secondary value indicators, including prior transactions, unexecuted purchase offers and buy-sell formulas.

You'll also need a valuation to comply with Financial Accounting Standards Board requirements for a business merger or acquisition — and on a post-M&A basis to test intangible assets for impairment. In addition, a valuation is handy for assessing life insurance coverage needs, as well as estate planning and filing an estate tax return as an owner's estate executor. Valuations can also help resolve disputes related to gift and estate taxation, shareholder agreements, divorce litigation, solvency or economic damage calculations.

Moreover, if you're converting your C corporation to an S corporation, a valuation will help

establish a basis for the company's common shares of stock and its potential "built-in gain," which may be subject to taxes if the business (or a portion of it) is sold within a prescribed holding period (which is five years for businesses that make S elections in 2013).

Methods used when valuing a business

Financial statements provide a useful starting point for valuing a business, but they reflect only historic values and operating results. More meaningful are the current market values of your assets and the economic benefits your business will provide in the future. To get a complete picture of your company's worth, valuators consider several internal variables, including its strengths and weaknesses, opportunities and threats, and tangible and intangible assets. External factors, such as economic and market conditions, also impact value.

Because the valuation process is so complex, it's critical to work with an accredited valuation professional skilled in selecting relevant valuation methodology. Not all appraisal methods apply to every business valuation assignment.

Under the *cost* or *asset-based* approach, business value is the difference between the combined value of assets and that of liabilities. It's quite useful to businesses — asset holding companies, for example — that rely on hard assets and possess few intangible assets.

The *income approach* determines the present value of a business's anticipated future cash flows, which are discounted at a rate of return on par with the company's risk. It's very useful when valuing service businesses with considerable intangible assets, as well as for businesses that generate positive cash flows.

Last is the *market approach*, which estimates pricing multiples from sales of similar private businesses or comparable public stocks. These multiples establish relationships between actual transaction prices and the comparables' economic performance — for example, price-to-earnings or price-to-sales. To obtain a meaningful sample of comparables, valuators use various selection criteria, including standard industrial classification code, transaction date and size.

Within each of these three basic approaches, there are various valuation methods that may be applied depending on the availability of data, your company's distinct characteristics, and the specific purpose of the valuation.

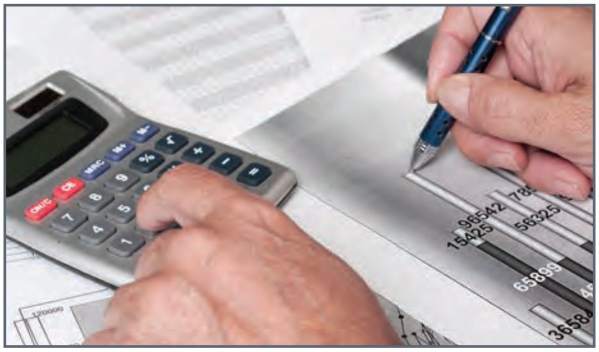
Less obvious indicators of value

Industry rules of thumb — such as one times revenues or five times earnings — spread like wildfire. These may *seem* simple, but the terms are ambiguous and the formulas tend to appraise everyone equally, regardless of financial performance and other differentiating qualities.

Always tell your valuator about rules of thumb and other secondary value indicators, including prior transactions, unexecuted purchase offers and buy-sell formulas. While they should *never* be the sole valuation method, secondary indicators can serve as useful sanity checks for the appraiser's conclusion.

Not as easy as it seems

As you can see, there's more to valuing a business than meets the eye. Because it's such a complicated process, it's critical that you retain a qualified valuator to appraise the business. ◈



6 ways to survive an IRS audit

The chances that an IRS agent will come calling with news that your tax return was chosen for an audit are mercifully low. Overall, about 1% of individual tax returns are audited each year, according to the *2012 Internal Revenue Service Data Book*. Of those, about three-quarters are correspondence audits that are handled by exchanging information via snail mail. The remainder, which are selected for field audits, are conducted by IRS officers.

Even though it's likely you won't experience an audit, knowing what might happen if your return is picked can help smooth the process. Here are six tips that can help you get through the audit.

1. Stay calm

Your tax return may have been chosen for examination randomly, or because the IRS needs more information. Receiving an audit notice doesn't mean you're suspected of cheating.

2. Don't ignore the IRS

Most notices include a deadline by which you're required to respond. Contact from the IRS about an audit will be made either via phone or mail with a follow-up letter. (The Service doesn't use e-mail to notify taxpayers of pending audits.) If you received a letter, the upper right corner should include a number specifying the reason for the correspondence. For instance, Notice Number CP05A indicates that the IRS is examining your return and needs documentation.

3. Gather information

Once you understand the focus of the IRS examination, begin gathering the information you'll need to respond appropriately. This may include invoices, canceled checks and receipts, as well as your tax return for the year(s) in question. Make duplicates of any documents you'll need to provide the IRS, so you don't hand over your only copy of a record.

While it's critical to provide the information requested, you generally don't want to offer additional data, such as tax returns from years falling outside the audit's scope. Doing so may prompt additional questions.

4. Consult a tax professional

Although it may be tempting to handle an IRS audit without paying for outside expertise, engaging a tax professional is worth the cost. The professional's experience with the audit process should enable him or her to know what information should be provided and how to answer questions appropriately, without inviting further investigation. The tax expert also can review any documents you're asked to sign — before you put pen to paper. This can be valuable whether you're responding in person or via a letter. Finally, having an expert on your side can limit the time and stress of the audit.

5. Expect some change to your return

IRS statistics for fiscal 2012 show that only 15% of correspondence audits with individual taxpayers resulted in no changes to the returns. For field audits, the percentage was 10%.

The numbers are more promising for corporations with assets of less than $10 million. Some 28% of these returns examined in field audits and 46% of correspondence audits resulted in no changes.

Although it may be tempting to handle an IRS audit without paying for outside expertise, engaging a tax professional is worth the cost.

If it becomes clear that you owe more, how much can you expect to pay? The average recommended additional tax per individual return for 2012, assuming income of less than $200,000, no Earned Income Tax Credit, and with Schedule E (Supplemental Income and Loss) or Form 2106 (Employee Business Expenses) was $3,379 for those handled via correspondence audits, and $9,922 for returns examined in field audits.

6. Resolve any differences

Most audited taxpayers agree to the changes proposed by the IRS. However, you can appeal the decision through the IRS's Appeals Office, or you can take your case to court. IRS Publication 5, *Your Appeal Rights and How To Prepare a Protest If You Don't Agree*, explains your rights to appeal and the proper procedures.

Avoid the pain

Although few taxpayers welcome an IRS audit, many can be handled without undue pain. Knowing what to expect and taking steps to prepare for the audit can make the process less worrisome and more efficient. Your tax advisor stands ready to help you if the IRS ever comes knocking at your door. ◈

Health care act may make HSAs more attractive

Health Savings Accounts (HSAs) allow you a tax-advantaged way to fund your health care costs. And the 2010 health care act may make HSAs even more attractive. Why? Because the act sets a higher threshold for deducting medical expenses.

What's the new floor?

The tax code allows you to deduct qualified medical expenses — such as for medical and dental services and prescription drugs — but only to the extent those expenses exceed the applicable threshold or "floor." Before 2013, that floor was 7.5% of adjusted gross income (AGI). Effective in 2013, the health care act has raised the floor to 10% of AGI.

That means it will be harder to exceed the floor. And, even if you do exceed it, your tax savings will be less than what it would have been with the 7.5% floor. For example, suppose your AGI is $100,000. In 2012, you'd have been able to deduct medical expenses in excess of $7,500. But in 2013, you can deduct only medical expenses in excess of $10,000. Say your medical expenses for the year are $12,000. In 2012, your deduction would have been $4,500. In 2013, your deduction will be only $2,000.

If you're age 65 or older, however, you can continue to enjoy the 7.5% floor through 2016. Regardless of your age, be aware that the threshold for alternative minimum tax purposes was 10% before 2013 and continues to be 10%.

How can an HSA help?

An HSA allows you to save taxes on medical expenses without meeting any threshold and regardless of your income level. It allows you to make pre-tax or tax-deductible contributions up to an annual limit. (See the chart "2013 HSA and HDHP limits" at right.) The account can bear interest or be invested, and you can then withdraw money tax-free to pay for qualified medical expenses. You can even carry over a balance from year to year.

There's a catch, however: You can contribute *only* if you're covered by a qualified high deductible health plan (HDHP). See the chart for the HDHP criteria.

Is an HSA right for you?

As you consider an HSA, keep in mind that, although HDHP deductibles are relatively high, premiums typically are lower than for lower-deductible policies. Depending on your income and your health, the combination of an HDHP and an HSA can be advantageous, especially with today's higher 10% medical expense deduction floor. ◈

2013 HSA and HDHP limits

	Individual	Family
HSA annual contribution limit	$ 3,250	$ 6,450
HSA catch-up[1] contribution limit	$ 1,000	$ 1,000
Minimum HDHP deductible	$ 1,250	$ 2,500
Maximum HDHP out-of-pocket costs	$ 6,250	$ 12,500

[1] Taxpayers age 55 and older may qualify to make these additional contributions.