



CYBER SECURITY

Ensure You're Prepared in Case of a Data Breach

IF YOU'VE ever experienced a data breach, you will know just how difficult it is to deal with and all of the ensuing issues that come to the fore.

If customer or employee data was exposed, most states have strict notification laws that you must follow. You will no doubt be trying figure out how to gird your network for a future attack, and also how to regain your company's perhaps sullied reputation.

Whatever the results of the breach, how you deal with the ensuing fallout can make or break your company's ability to get back on its feet.

The online security and risk news website CSO recently published a list of the worst things you can do in the wake of a breach, a list it based on a presentation by Michael Bruemmer of Experian Data Breach Resolution.

Below are eight things you should strongly consider.

1. Use external agencies' services

Sometimes a breach is too big to deal with in-house, and the type of breach may make that option an unwise one. So it's best to have external help available if needed. Incident response teams, such as those offered by Verizon Business, Experian, Trustwave or IBM – to name just a few – should at least be evaluated and considered when forming a business continuity/incident response plan.

2. Engage a lawyer

"Enlisting an outside attorney is highly recommended," Bruemmer said.

"No single federal law or regulation governs the security of all types of sensitive personal information. As a result, de-

termining which federal law, regulation or guidance is applicable depends, in part, on the entity or sector that collected the information and the type of information collected and regulated."

3. Designate a decision maker

"While there are several parties within an organization that should be on a data breach response team, every team needs a leader," Bruemmer said.

There needs to be one person who will drive the response plan, and act as the single source of contact to all external parties.

They'll also be in charge of controlling the internal reporting structure – in order to ensure that everyone from executives to individual response team members are kept updated.

4. Have a clear communications plan

Miscommunication can result in you mishandling a data breach, as it delays action and adds confusion.

The decision maker should be the one who also is the main source of information, particularly for your attorney.

Additionally, you should have a plan for communicating with customers, and if necessary the public and the media if you are large enough.

"Companies should have a well-documented and tested communications plan ... which includes draft statements and other materials to activate quickly. Failure to integrate communications into overall planning typically means delayed responses to media and likely more critical coverage," Bruemmer said.

5. Have remediation plans

Develop plans that address how to engage with customers and others once the breach is resolved, as well as the es-

See 'Policy' on page 2




CONTACT US

If you have any question regarding any of these articles or have a coverage question, please call us at:

ISU Curry Insurance Agency
 489 E. Colorado
 Pasadena, CA 91101
 Phone: 626-449-3870
 Fax: 626 449-5268
 License No. : 0588757



EMPLOYEE BENEFITS

FSA 'Use It or Lose It' Rule Partially Eliminated

THERE IS good news for your employees if you offer medical flexible spending accounts (FSAs), which allow them to put aside pretax funds to pay for medical-related expenses through the year. "Use it or lose it" has been partially eliminated.

The IRS and the Treasury Department have issued new regulations that will now allow employees to carry over up to \$500 in unused account balances into the following year.

Up until now, any remaining funds in these accounts were forfeited at the end of the year if unused or, if the employer adopted one, at the end of a grace period that lasted up to two-and-a-half months. Under the grace period, unused account balances can be carried over and used to pay health care expenses incurred in the first 2½ months of the next plan year.

An FSA allows you to contribute money to the account for costs not covered by insurance: deductibles, copays and coinsurance. In addition, you can use your FSA to pay for health care costs that health insurance doesn't cover.

The "use it or lose it" caveat has always been a sticking point for some considering opting into an FSA, and the new regulations should increase participation.

The modification "cuts back on wasteful year-end FSA health care spending by limiting the risk of forfeiture and in turn reducing the incentive to spend down as year-end approaches in order to avoid the losing the unused funds," the Treasury Department said.

The new regulations allow employers to choose either to allow employees to carry over up to \$500 into the next year or offer a 2½ month grace period to spend the remaining account funds.

An estimated 14 million American families now participate in health care FSAs, according to the Treasury Department.

This year, employees can contribute a maximum of \$2,500 per year to their FSA.

FSAs should not be confused with HSAs (health savings accounts), which are tax-advantaged medical savings accounts available to taxpayers who are enrolled in an HSA-qualified high-deductible health plan.

Funds contributed to an HSA are not subject to federal income tax at the time of deposit.

Unused amounts in one year can be carried over to following years and added to subsequent contributions.

In order to qualify for an HSA, the policyholder must be enrolled in an HSA-qualified high deductible health plan (HDHP), and must not be covered by other non-HDHP health insurance or Medicare, and cannot be claimed as a dependent on someone else's tax return.

The annual contribution limit for HSAs is \$3,330 this year for individuals, and \$6,550 for family coverage.

There was no exemption until the Affordable Care Act, which bars reimbursement for over-the-counter medicines, with the exception of insulin, without a prescription. ❖



Continued from page 1

As Crimes Increase You Need Security of a Cyber Policy

establishment of additional measures to prevent future incidents. If you make new investments in processes, people and technology to more effectively secure the data, finding ways to share those efforts with stakeholders can help rebuild reputation and trust.

6. Provide a remedy to customers

Customers should be put at the center of decision making following a breach.

This focus means providing some sort of remedy, including call centers where consumers can voice their concerns and credit monitoring if financial, health or other highly sensitive information is lost.

7. Practice regularly

Practice the plan with the full team. Bruemme recommends regularly updating and revising your incident response plan. "By conducting a tabletop exercise on a regular basis, teams can work out any hiccups before it's too late," he said.

8. Tap your cyber policy

The threats to businesses grow with each passing day as hackers shift their focus to smaller firms. A cyber policy can cover costs associated with a breach, including notification costs and any fines that the state may impose.

Call **ISU Curry Insurance Agency** to learn how a policy can protect your company. ❖

Produced by Risk Media Solutions on behalf of ISU Curry Insurance Agency. This newsletter is not intended to provide legal advice, but rather perspective on recent regulatory issues, trends and standards affecting insurance, workplace safety, risk management and employee benefits. Please consult your broker or legal counsel for further information on the topics covered herein. Copyright 2013 all rights reserved.

WORKPLACE SAFETY

Keep Your Office Accident Free During the Holidays

WHILE A time of joy, the holidays bring with them additional safety challenges in the workplace that can result in employee injuries.

More than 12,000 Americans are treated annually for falls, cuts, shocks and burns due to incidents involving faulty holiday lights, dried-out Christmas trees, and other holiday decorations.

Incidents of fires rise drastically during the holidays. Christmas trees are involved in more than 300 fires each year, resulting in an average of 10 deaths, 40 injuries and about \$7 million in property damage and loss. Make sure that your smoke detectors are working, and your fire extinguishers are fully charged and easily accessible.

Decorating the workplace can result in falls and dangerous tripping hazards. Try to avoid placing trees, gifts or freestanding decorations in busy areas where people might run into or trip over them.

Always use the proper step stool or ladder to reach high places safely. Before using a ladder, read and follow the manufacturer's instructions. Potential trips over cords or decorations and falls from a ladder are workers' compensation claims waiting to happen.

Also, make sure no decorations block exits, cover exit signage, or block access to fire safety equipment. Do not place any decorations in exit corridors or on sprinklers.

Safety tips

Decorations

Holiday decorations should create higher morale at the workplace, not hazards and potential for accidents and injuries, so take proper precautions. Choose artificial greenery made of fire-retardant materials for office decorating.

All decorations (including trees, wreaths, curtains/drapes, hangings, etc.) should be either non-combustible (not all artificial trees are), inherently flame-retardant (the label will say so), or have been treated with a flame-retardant solution.

Trees

- Consider an artificial tree, which poses less risk than a live one.
- Make sure a live tree has water at all times, so as not to

dry out and become a fire hazard.

- Live trees can be safer when sprayed with flame retardant.
- Live trees should be in a location that does not interfere with foot traffic. Do not allow blockage of your escape route – doorways, exits or pathways.
- Don't place trees near heating vents or space heaters, where they can dry out.
- Keep in mind trees can be top heavy, so use a sturdy stand.

Electric lights

- Before plugging in electrical decorations, check for broken or cracked sockets, frayed, loose or bare wires, or loose connections. Damaged sets may cause a serious electric shock or start a fire.
- Don't overload extension cords, which can overheat and start a fire. Extension cords have different ratings, so be sure to check before plugging in multiple-light string sets.
- If an extension cord is used in a busy area or crosses a walkway, secure with duct tape or cover with mats or carpet.
- Use indoor lights only indoors, and outside lights outdoors.
- Fasten outdoor lights securely to trees, buildings, walls or other firm supports to protect from wind damage. Don't mount or support light strings in any way that might damage the cord's wire insulation.
- Turn off all lights on trees and other decorations when you leave the workplace. Lights could short and start a fire.

Trimnings/Other decorations

- Use only non-combustible or flame-resistant materials. Choose tinsel, artificial icicles, plastic or non-leaded metals.
- Wear gloves while decorating with spun-glass "angel hair," which can irritate eyes and skin. A common substitute is non-flammable cotton. Both angel hair and cotton snow are flame retardant when used alone. However, if artificial snow is sprayed onto them, the dried combination will burn rapidly.
- When spraying artificial snow on windows or other surfaces, be sure to follow directions carefully. These sprays can irritate your lungs if you inhale them.
- Never place trimmings near open flames or electrical connections.
- Avoid using candles in the workplace.

Parties

- Alcohol: Avoid alcohol, but if you do serve it, limit the drinks per person and stop serving an hour before the end of the party.
- Holiday food preparation: Thoroughly cook and serve foods at proper temperatures. Refrigerate cooked leftovers within two hours at 40 degrees Fahrenheit or below.

Seasonal events and decorations for the workplace can be a fun way to help employees enjoy the spirit of the holiday season together. Just remember to keep safety in mind, and make sure proper safety precautions are observed at all times. ❖

ISU Curry Insurance Agency
wishes you a happy holiday





SEXUAL HARASSMENT

Deadline for Prevention Training Draws Closer

SINCE 2005, employers with 50 or more employees in California have been required to provide supervisors with sexual harassment prevention training every two years.

Because many companies conducted their first training that year, the end of 2013 marks another deadline for further training for those employers.

Also, a new law hit the books this year that expands the definition of sexual harassment, which you need to relate to your supervisors.

If you have more than 49 employees, then you are required to conduct two hours of interactive sexual harassment prevention training for supervisors within six months of hire or promotion, and every two years after that.

You have to train all staff with "supervisory authority," defined as anyone who has independent authority to:

- Hire, transfer, suspend, lay off, recall, promote, discharge, assign, reward or discipline other employees;
- Direct the work of other employees; and/or
- Resolve employee conflicts.

Another key portion of the law requires interactive training, meaning the session should be led by a qualified trainer and should include any or all of the following:

- Discussion,
- Role-playing,
- Question and answer session.

Topics should include at least the following to be effective:

- Teaching what is classified as sexual harassment under state and federal law.
- True-to-life examples of conduct that constitutes sexual harassment.
- Explaining what to do if sexual harassment is witnessed.

- Steps employees can take to report harassment.
- Training on what to do if an individual is personally accused of sexual harassment.
- Sexual harassment prevention methods.

Your training should also reflect changes to the definition of sexual harassment brought about by the signing into law of SB 292 this year.

That law expands the definition of sexual harassment to include conduct that is not motivated by sexual desire.

The legislation was in response to a recent Appeals Court ruling that rejected a claim by a male union apprentice ironworker who was subjected to sexually explicit comments regarding his body and threats of sexual acts by a supervisor.

The court held that since the record showed that the supervisor did not harbor a true desire to have sex with the apprentice, his abusive language and behavior could not be considered sexual harassment.

Regardless of whether you conduct the training in-house or use a vendor, make sure that you keep records of the training, the provider of the training and the date of the session for all of your supervisors.

Have everybody who is trained sign documents indicating they underwent the training.

Also, make sure that you give all employees a copy of your policies on sexual harassment, in addition to a sexual harassment information sheet on an annual basis at a minimum. ❖



State Compensation Insurance Fund to Hike Its Rates



IN A MOVE that reflects the overall pricing trending in the market, State Compensation Insurance Fund is planning to increase its overall rates by 6.5% in January 2014.

State Fund had actually reduced its rates by 7% at the start of 2013 in anticipation that claims costs would fall after last year's workers' comp reforms took effect.

According to reports in the trade press, State Fund also plans to hike its rates further in March 2014 and make changes to its group plans. The insurer said it is increasing rates to account for higher

claims costs and an increase in the average number of claims filed.

Meanwhile, for January 2014, State Fund has decided to reduce the premium discount of its Farm Bureau group to 6% from the current 20%. Other groups' discounts will remain as they are.

Also, State Fund's board has asked the insurer's management to analyze how group discounts are performing under the company's new tiered rating program, according to the *Workers' Comp Executive* newsletter.

State Fund will also conduct a review of its safety groups' safety and other outreach efforts to make sure they are in compliance with the insurer's overall group agenda.

And in March, State Fund plans to increase minimum premiums and raise rates further, according to the *Executive*. ❖