May 2015 Volume 3, Issue 9

Curry Insurance Agency

CYBER SECURITY

Threat Grows with Human Error, Ransomware

NEW RESEARCH shows two big trends in the busy area of cyber security: careless employees are a prime reason many companies' databases are getting "phished" for data; and the rising tide of ransomware, where hackers freeze up a computer and demand payment to release it.

Easy entrance

When these malicious code-bearing e-mails (phishing and ransomware alike) are sent, there is an 11% chance that an employee will click on the link that will let the phishing program gain entry into your database, according to the Verizon "Data Breach Report." If 10 employees receive such an e-mail, there is greater than a 90% chance that one of them will click on it.

Even worse, 50% of users open e-mails and click on phishing links within the first hour.

In a more disturbing trend, the "Internet Security Threat Report" by Symantec Corp. noted that 60% of all targeted attacks strike small and medium-sized organizations.

"These organizations often ... are still not adopting basic best practices like blocking executable files and screensaver e-mail attachments. This puts not only the businesses, but also their business partners, at higher risk," Symantec wrote in its report.

Phishing

Phishing is an attempt to gain access to a database by masquerading as a trustworthy entity in an electronic communication. Phishing campaigns have evolved in recent years to incorporate installation of malware as the second stage of the attack.

In phishing, tainted e-mails are sent to employees and if just one person clicks on the link, it allows hackers to gain entry into the company's database.

This allows the hackers to root through the database to acquire sensitive information such as user names, passwords and credit card details (and sometimes, indirectly, money).

While phishing was fading in 2013, it made a resurgence in 2014 largely thanks to employees clicking on links in bogus e-mails.

This human-error dynamic is a significant frustration for businesses that erect firewalls and use other methods to protect their data.

See 'Ransomware' on page 2

CONTACT US

Curry Insurance Agency

If you have any questions 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

Paid Sick Leave Law Starts on July 1

CALIFORNIA'S PAID sick leave law takes effect July 1 and if you haven't begun preparing for this change, you should start now. If you don't you may run afould of state wage and hour laws, exposing you to legal action.

Even if you already provide paid sick leave for your staff, you should familiarize yourself with the new law.

The California Chamber of Commerce recommends the following for employers in the Golden State:

What you should be doing now

- Post the new paid sick leave notice in a place where staff can easily see it.
- Provide the updated wage theft notice to nonexempt employees.
- Check if there's a local ordinance for paid sick leave.
- Review your existing policies for sick leave.
- Ensure your policies cover all eligible staff, for all permissible uses.
- Choose which method you'll use to provide paid sick leave benefits to employees – accrual, lump sum or existing policy.
- Communicate your paid sick leave policy to your staff.
- Train supervisors about specific paid sick leave rights for employees.
- Update your payroll systems to track sick leave.

On July 1 and after

- Begin providing paid sick leave benefits to employees who have worked for more than 30 days, or after 90 days of being hired.
- Follow the law's requirements regarding usage, record-keeping and timely payment.
- Track paid sick leave and show how many days of leave an employee has available, either on a pay stub or on a written document issued the same day as the paycheck.

Continued from page 1

Ransomware Also Gains Foothold from Careless Clicks

Ransomware

The other growing threat is ransomware (also the result of clicking on tainted e-mails). Once someone clicks on a link, malware infects the computer system and freezes some or all functions.

After the system is rendered unusable, the company will receive a ransom e-mail telling it to pay a certain amount to unlock its computers.

Ransomware attacks more than doubled in 2014 to 8.8 million, from 4.1 million in 2013, according to Symantec. Put another way, there were 24,000 attacks per day, compared with 11,000 in 2013.

But there is a worse threat in the ransomware category: crypto-ransomware. It encrypts your personal files and holds the keys to their decryption for ransom at a remote site.

What you can do

Find ways to bird-dog malicious e-mails before they reach in-boxes. The methods that will give you the most bang for your buck are:

- Better e-mail filtering before messages arrive in user in-boxes.
- Developing and implementing a thorough security awareness program from the top to the bottom of your organization. That means including training on how to spot suspicious e-mails, quarantining them and resisting the urge to open e-mails from familiar-sounding names of people you don't know.
- Improved detection and response capabilities.

The preferred method is to take measures to block, filter and alert on phishing e-mails at the gateway.

That said, no technological defense is foolproof, so your people are really your last line of defense.

One of the most effective ways you can minimize the phishing threat is through effective awareness and training.

One idea is to teach all staff to be your scouts and if one of them detects a suspicious e-mail, they can send it to your head of IT or a manager, who can decide to send out a warning to all the staff.

Basically, you create a network of human sensors that are more effective at detecting phishing attacks than almost any technology. ❖

Ramp up Training on Cal/OSHA's New Heat Illness Standard

CAL/OSHA has made significant revisions to the California heat illness standard, which will take effect for the 2015 summer.

The Cal/OSHA board has approved an early implementation of May 1, so the changes are in place for the upcoming growing season.

That means that you need to revise your firm's heat illness program and train your workers and supervisors in a hurry.

The revisions mainly focus on the provision of water and shade. They also tighten up high-heat provisions and add new language on emergency response procedures, acclimation and training.

This standard applies to all outdoor places of employment. The following industries are subject to additional requirements in high heat (95° F or above):

- Agriculture,
- Construction,
- Landscaping,
- Oil and gas extraction, and
- Transportation and delivery of agricultural products, and of construction or other heavy materials. ❖

New rules: water, shade, high heat

Water

Water must be "fresh, pure, and suitably cool" and located as close as practicable to where employees are working, with exceptions when employers can demonstrate infeasibility.

Shade

Shade must be present at 80 degrees, instead of the current 85, and accommodate all employees on recovery or rest periods, and those on-site taking meal periods.

Monitoring

Employees taking a "preventative cool down rest" must be monitored for symptoms of heat illness, encouraged to remain in the shade and not ordered back to work until symptoms are gone. Employees with symptoms must be provided appropriate first aid or emergency response.

High-heat procedures

High-heat procedures (triggered at 95 degrees) shall ensure "effective" observation and monitoring, including a mandatory buddy system and regular communication with employees working by themselves. During high heat, employees must be provided with a minimum 10-minute cool-down period every two hours.

Emergency response

Emergency response procedures include effective communication, response to signs and symptoms of heat illness and procedures for contacting emergency responders to help stricken workers.

Acclimation

Acclimation procedures include close observation of all workers during a heat wave – defined as at least 80 degrees.

Confused? Contact us. We can help!

WORKPLACE SAFETY

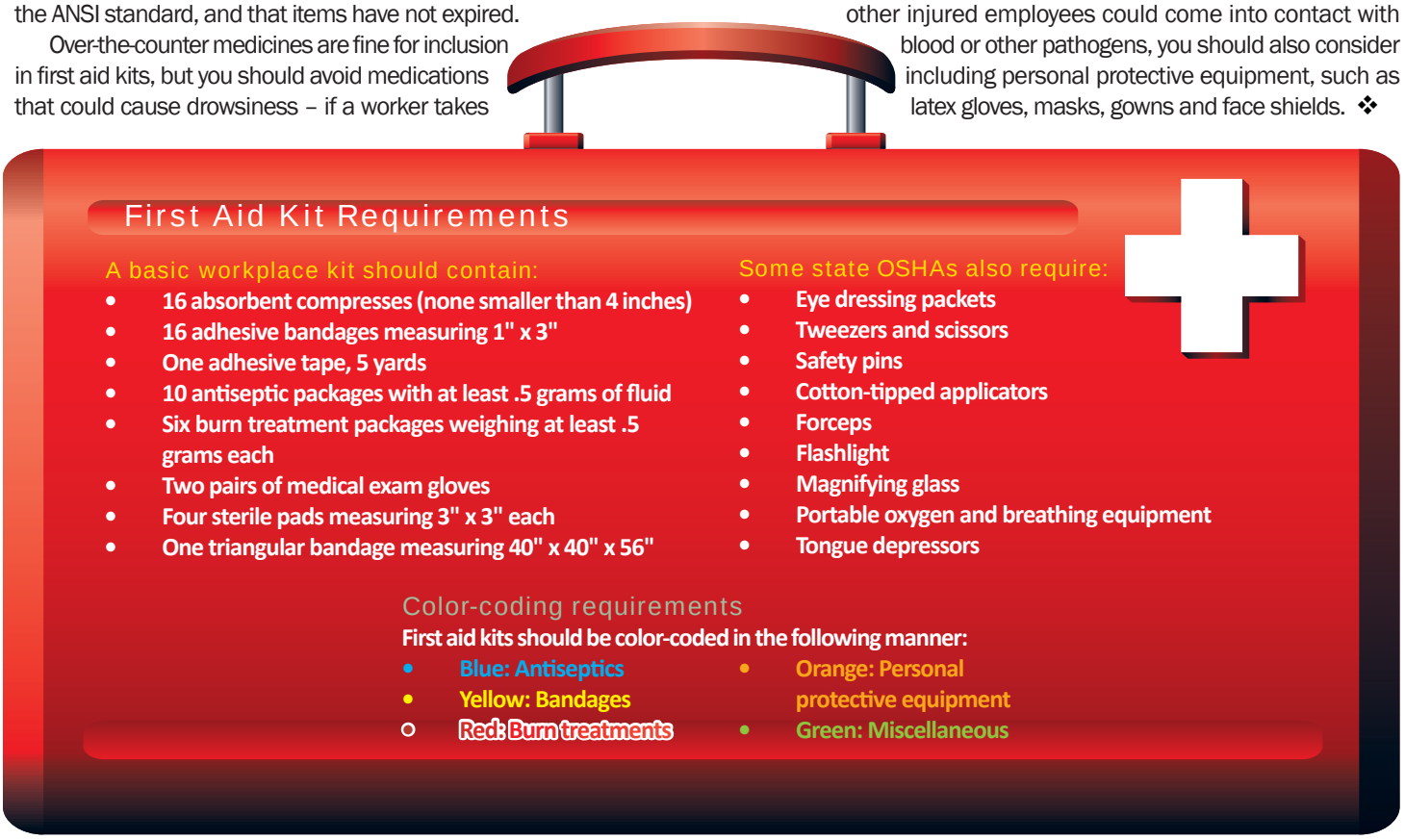
Essentials of an OSHA-approved First Aid Kit

DO YOU know what OSHA requires you to keep in the first aid kits at your place of business? Fed-OSHA Standard 1910.151 requires that "adequate first aid supplies shall be readily available."

You should put a staff member in charge of inspecting first aid kits on a regular basis to make sure they have all the items required under the ANSI standard, and that items have not expired.

Over-the-counter medicines are fine for inclusion in first aid kits, but you should avoid medications that could cause drowsiness – if a worker takes one of these and has an accident soon afterwards, the implication could be that you as the employer may be culpable.

If you do include over-the-counter medications, all meds should be wrapped in tamper-evident packaging as individual doses. You should not have any bottles. If you reasonably expect that workers treating other injured employees could come into contact with blood or other pathogens, you should also consider including personal protective equipment, such as latex gloves, masks, gowns and face shields. ❖



First Aid Kit Requirements

A basic workplace kit should contain:

- 16 absorbent compresses (none smaller than 4 inches)
- 16 adhesive bandages measuring 1" x 3"
- One adhesive tape, 5 yards
- 10 antiseptic packages with at least .5 grams of fluid
- Six burn treatment packages weighing at least .5 grams each
- Two pairs of medical exam gloves
- Four sterile pads measuring 3" x 3" each
- One triangular bandage measuring 40" x 40" x 56"

Some state OSHAs also require:

- Eye dressing packets
- Tweezers and scissors
- Safety pins
- Cotton-tipped applicators
- Forceps
- Flashlight
- Magnifying glass
- Portable oxygen and breathing equipment
- Tongue depressors

Color-coding requirements

First aid kits should be color-coded in the following manner:

- Blue: Antiseptics
- Yellow: Bandages
- Red: Burn treatments
- Orange: Personal protective equipment
- Green: Miscellaneous

A Word about Automated External Defibrillators

WHILE OSHA does not require on-site defibrillators in the workplace, some employers may decide to have one on hand.

With recent advances in technology, automated external defibrillators (AEDs) are now widely available, safe, effective, portable and easy to use.

These devices provide the critical and necessary treatment for sudden cardiac arrest.

Using AEDs as soon as possible after sudden cardiac arrest, within three to four minutes, can lead to a 60% survival rate.

CPR is also important because it supports the circulation and ventilation of the victim until an electric shock delivered by an AED can restore the fibrillating heart to normal.

All worksites are potential candidates for AED programs because of the possibility of heart attack and the need for timely defibrillation.

Each workplace should assess its own requirements for an AED program as part of its first-aid response. ❖