PIASC Native.news

Download & print individual articles: http://bit.ly/NN-10-15-18

Published by Printing Industries Association, Inc. of Southern California

October 15, 2018 Issue 15

Legislative Roundup

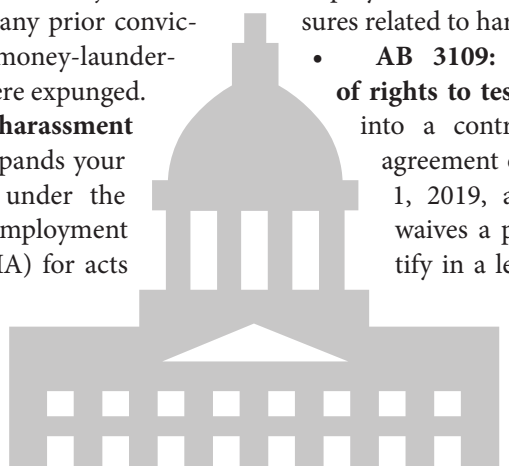
We've been keeping an eye on a variety of legislation as it makes its way through the California legislature. Now that this year's legislative session has come to an end, here's an update on what was signed into law…and what was not.

Signed into Law

• **SB 826: Female corporate board membership** – Requires publicly held corporations with principle offices in California to have at least one female on their Board of Directors by December 31, 2019; this increases to two or three females (depending on the overall size of the Board) by December 31, 2021. This law is expected to be challenged almost immediately on equal-protection grounds and is likely to face an uphill battle in court.

• **SB 1412: Job applicant criminal history inquiry** – If you use criminal background checks to screen job applicants, you must be careful when looking at expunged or judicially sealed convictions. Under this law (which is in addition to the rules you must follow under AB 1008, the "Ban the Box" ordinance), you may only consider these types of convictions in situations where conviction of that crime legally prohibits someone from holding the job in question. For example, an applicant for a job with a bank cannot have any prior convictions of fraud or money-laundering, even if they were expunged.

• **SB 1300: Sexual harassment omnibus bill** – Expands your potential liability under the California Fair Employment Housing Act (FEHA) for acts committed by nonemployees to all types of harassment, not just sexual harassment as under current law. Prohibits you from requiring employees to sign a release of claims under FEHA in exchange for a raise or bonus, or as a condition of employment. Prohibits you from requiring an employee to sign a non-disparagement agreement or other document that may deny the employee the right to disclose information about unlawful acts in the workplace, including sexual harassment. Authorizes—but does not require—you to provide bystander intervention training to your employees. And includes other measures related to harassment as well.



• **AB 3109: Banning waivers of rights to testify** – If you enter into a contract or settlement agreement on or after January 1, 2019, any provision that waives a party's right to testify in a legal proceeding regarding criminal conduct or sexual harassment on the part of the other party is void and unenforceable.

• **SB 820: Settlement agreement provisions** – If you enter into a settlement agreement on or after January 1, 2019, any provision that prevents the disclosure of information related to complaints of sexual assault, sexual harassment, workplace harassment or discrimination based on sex is void and unenforceable. However, at the claimant's request, the agreement can include a provision that shields the claimant's identity.

• **SB 1343: Workplace sexual harassment training** – Extends the requirements to provide workplace sexual harassment training to employers with just five or more employees. Mandates that this training be provided every two years to all employees, both supervisory and non-supervisory. Beginning in 2020, mandates that this training must also be provided to seasonal and temporary workers.

To make it easier to provide this training, the law also requires the Department of Fair Employment and Housing to develop one- and two-hour online training courses and make these courses available on the agency's website.

• **AB 1976: Workplace lactation accommodations** – Requires you to make a reasonable effort to provide a room "other than a bathroom" (not just "other than a toilet") to accommodate lactating employees.

Continued on back

BUSINESS MANAGEMENT

Can Your Business Survive a Cyberattack?

Major cyberattacks on major companies have become so commonplace that they're no longer shocking or surprising. What is surprising, though, is how many owners of smaller businesses think that this can never happen to them. "I'm just a little guy," they think. "Why would the bad guys waste their time going after my system?" Then they get hit with malware or ransomware, and they realize that small businesses are targets, too.

Why cybersecurity needs to be on your radar

Your business is powered by digital technology. In some shape or form you rely on computers every day, for pretty much everything. If something happens to your computer systems—if they get knocked out by a virus, or if you get locked out by ransomware—your business will grind to a halt.

On top of that, you trust that the vital data, knowledge, personal information and trade secrets that you store on this digital technology is all safe and secure. Your customers trust that the digital files they submit to you are safe and secure. Your employees trust that their employee records, including their social security numbers, are safe and secure. And so on.

But the bad guys know better. They know that most small and medium-sized businesses (SMBs) either take a laissez-faire approach to cybersecurity or simply do not have the skills or funds to put strong cybersecurity measures in place. They're aware of these vulnerabilities. They also know that SMBs have a lot of data stored in their computer systems that, at a minimum, is extremely valuable to that business (hence the growth of ransomware) and is often valuable on the open market as well.

So, it's no wonder that smaller businesses are frequently hit with cyberattacks. In fact, according to a 2017 report from the Ponemon Institute (see http://bit.ly/stateofcybersecurity, 61% of small businesses surveyed experienced at least one cyberattack in 2017.

There are two main types of cyberattacks

When cyber criminals attack your system, they usually have one of the following goals in mind:

• **Steal your data** – Malware and phishing

• **Stop your ability to do business** – Ransomware, "denial of service" attacks

• **Both of the above** – Steal your data plus encrypt it and charge a ransom to return access to you

Basic cybersecurity measures for your business

Knowing all of this, the question becomes, "What can I do to protect my company?" The best cybersecurity plans have multiple layers. We asked a cybersecurity professional, Rene Kolga, Product Manager for cybersecurity software maker Nyotron, to provide our members with some recommendations regarding what these multiple layers should be. Kolga recommends that at a minimum you should start with the basics…

• **Require long passwords** – While we used to talk about password complexity (i.e. passwords with special characters, numbers and both upper and lower case letters), it has now been proven that length is more important than complexity. A 10- or 12-letter lower case password that consists of a few words merged together is exponentially harder to crack than a complex 6- or even 8-character password.

• **Use multi-factor authentication** – Require the use of more than one thing in order to obtain access to your system. Two-factor authentication usually combines passwords with something else, such as a one-time code sent via text or email.

• **Train your employees** – Your employees will always be the weakest link in your cybersecurity program. From weak or reused passwords to clicking on malicious links to installing problematic apps, your employees' poor habits can unwittingly open the door to cyber threats. For a list of some of the things this training should include, see our previous article at http://bit.ly/NN-6-25-18

• **Stay current with software updates** – As Kolga says, "Patch early and patch often! Cyber criminals will take advantage of any known vulnerabilities in your software; the updates and patches will address the majority of these vulnerabilities. Keep all of your applications up-to-date, from your operating system and Microsoft Office suite to your graphics programs, web browsers, accounting system, CRM and whatever else you are running on-premises."

Of course, this isn't an issue with cloud-based Software as a Service (SaaS) applications, such as Office 365, as these are kept up-to-date by the provider.

• **Create secure backups** – To protect against loss of data, having good backups in place is absolutely critical. But it's not enough to just backup your data, because the first thing most of the sophisticated ransomware programs will do is look for and corrupt or delete your backup.

It is best to back up to an off-site facility that is not physically connected to your system. For disk-to-disk backups done on premises, be sure to physically remove the disk from the system each day. Ensure that if your system is attacked by malware or ransomware, your backup will not be accessible to the attackers.

• **Practice recovering from a backup** – "The most important thing about backups," states Kolga, "is the restore. Having a secure backup won't do you any good if you cannot recover from it." Run practice drills to be sure you can actually fully recover from a backup if all of your primary data is wiped out.

• **Install multiple layers of protection on your systems** – Today's cybersecurity products are all based on one of two different approaches: "Negative Security" and "Positive Security."

Products based on the "Negative Security" model focus on trying to find the

Continued on back

RISK MANAGEMENT

Harassment Claims Can Come from Unexpected Sources

A recent study of workplace harassment highlights the pervasive nature of workplace harassment. In fact, 35% of the respondents in this survey—and 41% of women respondents—stated they had been harassed at work at some point in their career.

While the #metoo movement has shined a spotlight on sexual harassment, which accounts for more than half of harassment incidents, other types of harassment are common as well.

Harassment isn't just the stuff you'd expect

At this point you most likely know that it is illegal for one of your supervisors to make unwelcome sexual advances towards a subordinate. But you might not have realized that situations like the following two examples could result in lawsuits as well:

• **Sales rep harassed by client** – A new sales rep, Martha, calls on one of the company's biggest customers. While there the customer's President, Jarod, makes some sexually-charged remarks. When she gets back to her office Martha tells her supervisor what happened. "Oh, don't worry about it," she is told. "Jarod is harmless."

On her next visit to this client, Jarod squeezes Martha's thigh and suggests there's an "easy way" for her to "get a big order." Martha pushes his hand away and leaves. Back at her office Martha's supervisor reminds her that this is one of the company's biggest clients. Instead of taking action to stop the harassment, the supervisor offers to remove Martha from the account, which would deprive her of significant potential commissions. Martha responds by filing a harassment suit.

• **Assistant who divulged confidential information** – The Executive Assistant to the Chief Financial Officer was terminated for divulging confidential information to staff regarding impending company layoffs. Given the fact that she clearly did something unacceptable, the company assumed that would be the end of the story. It was not. The now-former employee filed a lawsuit for retaliation and sexual harassment, claiming that the CFO always made suggestive comments and had improperly touched her (something she hadn't previously mentioned). Defending the CFO in this real-life example cost over $150,000.

Not all harassers are bosses or men

Another finding of this workplace survey was that 73% of the people who claimed to have been harassed said they were harassed by someone who was in a senior position to them in the organization, and 78% said their harassers were men. While these figures are quite high, they are less than 100%. The implication is that 22% of harassers are women, while 27% are peers, subordinates, customers or vendors. And even in situations where the harasser is not an employee, the employer can still be liable if they fail to stop reported harassment.

Harassment often goes unreported…for a while

Victims of harassment are often afraid to come forward.

• 53% fear that a hostile work environment will be created

• 46% fear retaliation from their employer

• 39% fear management won't handle the situation properly

• 33% fear retaliation from the harasser(s)

However, what we've seen is that a lot of claims are filed by people who have been fired or laid off. This is most likely because at that point these people probably feel like they've got nothing to lose. If they've already lost the job, a hostile

Continued on back

Upcoming Events

Toy Drive & Ride

October 1st – November 26th

If your company is looking to give back, think of the kids at City of Hope. This year, our goal is to put smiles on hundreds of kids' faces. Make a difference this holiday season and participate in our annual Toy Drive, which now includes a ride to deliver all the gifts.

If you agree to participate, PIASC will send you a box for donations. Once you reach 20 gifts, your logo will also be included in all promotional items as a sponsor.

Donate by Monday, November 26, 2018. Drop-off location:
5800 S. Eastern Ave, Suite #400
Los Angeles, CA 90040
(Bank of America Building, 4th Floor.)

To participate in the Toy Drive contact Maribel Campos at maribel@piasc.org or 323.728.9500 ext. 210.

Committed Sponsors: The Dot, GPA, Specialty Substrate

Group Motorcycle Ride

Saturday, December 1st

You can also join the GROUP MOTORCYCLE RIDE to deliver donations… All Bikes are welcome and Santa outfits highly suggested!

Starting Point: GPA Specialty Substrate Solutions, 16001 Arthur St, Cerritos, CA 90703

Check-in begins: 8:00am

Ride to City of Hope: 9:15am (Kick Stands Up)

Destination & Distribution of Gifts: City of Hope, 1500 E. Duarte Rd, Duarte, CA 91010

To join the ride contact Bill Rivera at (949) 422-8330

FEATURE ARTICLE

Continued from front

• **AB 2334: Cal/OSHA recordkeeping** – As an employer you are required to record workplace injuries and illnesses in your OSHA Form 300 Log. Starting January 1, 2019, you will be on the hook for record-keeping violations well beyond the federal six-month statute of limitations. A failure to record an injury or illness will now be deemed a "continuing violation" until it is discovered by Cal/OSHA, corrected by you, or reaches a point where the duty to maintain the record no longer exists.

• **AB 1753: Controlled substances Rx forms** – Reduces the number of printers approved to print prescription forms for controlled substance prescriptions from about 40 currently to just three statewide.

Vetoed by Governor Brown

• **AB 3080: Non-disparagement clauses and mandatory arbitration agreements** – Meant to address two legal tactics commonly used in relation to employment contracts that have been used to silence victims and witnesses of workplace sexual harassment.

• **AB 3081: Workplace sexual harassment** – Would have prohibited certain types of discrimination against employees who are victims of sexual harassment and would have required employers and labor contractors to share responsibility and liability for all workers supplied by that labor contractor.

• **AB 1867: Sexual harassment record keeping** – Would have required employers with 50 or more employees to retain records of internal sexual harassment complaints for five years from the separation date of the complainant or the alleged harasser, whichever date was later.

• **SB 937: Workplace lactation accommodation** – There were two bills regarding workplace lactation accommodations. AB 1976 was signed into law, while SB 937, which was extremely specific regarding the exact nature of the lactation accommodations to be provided, was vetoed.

• **AB 1870: Employment practice claims timing** – Would have extended the period during which employees can file complaints with the California Department of Fair Employment and Housing from one year to three years.

RISK MANAGEMENT

Continued from front

work environment, retaliation, etc. are no longer concerns.

Prevention, early detection and proper insurance coverage are all key

Even if there is no settlement or award, simply defending your company against harassment lawsuits can be extremely costly. To avoid this, and to maintain a respectful and successful workplace, you should:

• **Provide legally-mandated anti-harassment training** and enforce a "zero-tolerance" policy regarding harassment.

• **Create a responsive and open organization** that allows employees to share their experiences with no threat of retribution.

• **Watch for patterns of behavior** that might indicate harassment.

• **Take reports seriously** and address allegations and rumors immediately.

• **Conduct anonymous employee surveys** that include questions about any harassment that employees have seen in your workplace.

• **Have Employment Practices Liability Insurance (EPL) in place.** This type of policy provides coverage for harassment and other Employment Practices Violations. To learn more about Employment Practices Liability Insurance, contact PIASC Insurance Services today at 323.728.9500.

BUSINESS MANAGEMENT

things that are bad—viruses, malware, ransomware, corrupted files, etc.—and then deleting or quarantining the offending items. Most end-point security products installed on laptops, desktops and servers, including all of the popular anti-virus programs, use this approach. This type of product is an excellent choice for your first line of defense.

Products based on the "Positive Security" model do the opposite. These products know what is good, only let these good things in and block out everything else. Nyotron's product, PARANOID (see https://www.nyotron.com/solutions/paranoid/) is a great example of this. Because all applications run on top of the operating system (OS), PARANOID is based on the "good behavior" of the OS. Anything that falls outside of this "good behavior" is assumed to be "bad," and is therefore blocked. It's a threat-agnostic, user-agnostic, application-agnostic approach.

"We always recommend that organizations use multiple layers of cybersecurity," Kolga states. "Think of it like protecting your home. If you can stop a burglar with a good lock, that's great. But just because a skilled locksmith can unlock that door in 30 seconds doesn't mean that you should remove the lock or the door. They're still good deterrents. Instead, you should add additional layers of security on top of that. Positive Security-based products are that next level of security for your IT system."

Conclusion

One other thing to keep in mind is that it is your legal responsibility to safeguard Personally Identifiable Information and Protected Health Information ("PII" and "PHI" data). Plus, of course, when it comes to data breaches, your company's reputation is on the line. Given the fact that many organizations are now experiencing near-continuous cyberattack attempts, if you have not already done so, getting cybersecurity in place is a must!

HUMAN RESOURCES

Sample Equal Employment Opportunity Policy Released

Under California law, employers have an affirmative duty to attempt to prevent—and to promptly correct—any conduct that is discriminatory and/or harassing. In addition, employers are also required to have a written anti-discrimination, anti-harassment and anti-retaliation policy that satisfies very specific legal requirements.

The California Department of Fair Employment and Housing (DFEH) recently released its Sample Equal Opportunity Policy, which you can use as a guide when reviewing or updating your existing policies.

Action item: Download the Sample Policy and compare it to your existing policy. Update your policy as needed.

New FMLA Forms Now Available

The Department of Labor (DOL) has issued new Family and Medical Leave Act (FMLA) medical certification and notice forms. These are substantially identical to the old forms, which have now officially expired, with the exception of a new August 31, 2021 expiration date.

The updated forms can be found at http://bit.ly/fmlaforms.

Action item: Download the new forms and use them to replace the old forms. FMLA compliance can be a treacherous regulatory minefield. Using the official forms is one way to ensure all appropriate documentation is created.

Other Industry Events 2018-2019

10/15/18 - 10/17/18	Adobe MAX	Los Angeles, CA		www.max.adobe.com
10/18/18 - 10/20/18	2018 SGIA Expo	Las Vegas, NV		www.sgia.org/expo/2018
10/25/18	Think Bowl: Ghouls and Gutters	Westchester, CA	olivia@thinkla.org 310.876.0650, x226	www.thinkla.org
10/30/18 - 10/31/18	2018 OSHA Compliance for Printing Workshop	Warrendale, PA	412.259.1779 krundle@printing.org	www.printing.org
11/13/18	ETHOS: 2018 Design Annual	Costa Mesa, CA		www.orangecounty.aiga.org
4/4/19 - 4/9/19	2019 AIGA Design Conference	Pasadena, CA		www.orangecounty.aiga.org

Want us to list your event? Contact Maribel Campos, 323.728.9500, Ext. 210, maribel@piasc.org

CONTACT US

Address:
5800 S. Eastern Avenue, Suite 400
Los Angeles, CA 90040

P.O. Box 910936
Los Angeles, CA 90091

Phone: 323.728.9500
www.piasc.org

Key Contacts

Lou Caron, President
Ext. 274, lou@piasc.org

Dennis Bernstein, Commercial Insurance
Ext. 222, dennis@piasc.org

Evie Bañaga, Employee Benefits
Ext. 224, evie@piasc.org

Kristy Villanueva, Member Services
Ext. 215, kristy@piasc.org

Cheryl Chong, Human Resources
Ext. 218, cheryl@piasc.org

Irv Selman, Individual Insurance
Ext. 249, irv@piasc.org

CLASSIFIEDS

FOR SALE HP 5500 Designjet for $995.00. Barely used. Contact amorton@cdsop.com, almorton@socal.rr.com or 714-767-4443

FOR SALE Xerox Versant 180 Assume remaining term on lease through 12/30/20. Monthly payments: $709.96 Versant, $537.43 Freeflow Print Server. Contact Ed at 714-229-9700

FOR SALE Soda Vending Machine - 8 Spots Great condition. Paid $800, will sell for $400 OBO must pick up in Gardena. Contact Rose 310-638-7768 X11 or email rose@RNJprinting.com

FOR SALE Hamada B452A 14x20 4 color press. 2001 machine with 35mm impressions, top condition with less than 500m on all new rollers, auto plate hangers, Piery infrared drier, refrigerated water system, all manuals and tools, viewing station. Runs metal or poly plate. Can be seen running locally. DPX available. Ask for Kristy Villanueva, 323.728.9500, kristy@piasc.org

Want to place a classified ad? Contact Erica Sanchez, 323.728.9500, Ext. 209, erica@piasc.org

PIASC Events Calendar

OCT. 1 – NOV. 26
Toy Drive & Ride
Drop-off Location: PIASC Offices, Los Angeles
Contact: Maribel Campos, Ext. 210, maribel@piasc.org to have a donation box delivered to your offices.

OCT. 30
WEBINAR: Selling Value in a Commodity-Driven Market
11:00 am – 12:00 pm, PDT FREE/members
Details: www.piasc.org/events
Contact: Emily Holguin, Ext. 262, emily@piasc.org

NOV. 14
WEBINAR: Critical Thinking
12:00 pm – 1:00 pm, PDT
FREE/members
Details: www.piasc.org/events
Contact: Emily Holguin, Ext. 262, emily@piasc.org

NOV. 15
Inkjet Ready! Part 2 Virtual Conference
10:00 am – 2:00 pm, PDT
$99/members
Details: www.piasc.org
Contact: Emily Holguin, Ext. 262, emily@piasc.org

DEC. 1
Toy Drive & Ride: Group Motorcycle Ride
8:00 am – 10:00 am,
GPA, Specialty Substrate Offices,
Cerritos to City of Hope, Duarte
Contact: Bill Rivera, 949.422.8330

For full list of workshops and virtual classes, please visit www.piasc.org/training.