PACIFIC DIVERSIFIED
INSURANCE SERVICES, INC.

THE REPORT

June 2017
Volume 5
Issue 3

REDUCING INJURIES

Getting Buy-in from Managers on Safety Programs

ONE OF THE keys to instituting a good safety program is to get management buy-in.

You need their support and belief in the system if you are to convince your employees to embrace your safety regimen.

If your managers don't believe in the safety plans you have put together, it will show through when they try to sell them to your staff.

If you don't have buy-in from your managers, the chances are slim to none that your employees will embrace the changes you are proposing.

If you are serious about preventing injuries and want to keep your workers' comp X-Mod low, the role of your management team is crucial.

You will often encounter a few different personality types among your managers and they need to be convinced of the importance of workplace safety in different ways.

You'll need a different approach with each personality type to get them to embrace the concept.

Once they do, they can effectively convey the urgency and importance of workplace safety to the rank and file.

Constructor Magazine has these recommendations for getting management buy-in:

Select the right leaders

Choose managers who are firm, yet fair with a passion for the safety of the workforce. They should have a track record of success so that they can be an inspiration to their teams. Also, they should not be afraid to get their hands dirty to make a point or demonstrate how something is done.

See 'Operation' on page 2

Safety personality types

The excuse-makers: They are the ones that blame external factors that are out of their control for safety lapses, and they may pooh-pooh the harm that a high X-Mod causes. They may talk the talk on safety, but they don't walk the walk.

Half-hearted bosses: These managers may actually buy into the safety program, but they are unable to show their commitment in ways that make an impression on the rank and file.

Committed: These managers are fully committed and enthusiastically embrace your safety plans and discuss them with staff with exuberance.

CONTACT US

Pleasant Hill Office
200 Gregory Lane, Bldg A
Pleasant Hill, CA 94523
Phone: 925-686-2860

Morgan Hill Office
15005 Concord Circle
Morgan Hill CA 95037
Phone: 408-842-2131

Elk Grove Office
2362 Maritime Drive, Suite 110
Elk Grove, CA 95758
Phone: 916-970-2745

San Diego Office
990 Highland Drive, Suite 110 C
Solano Beach, CA 92075
Phone: 858-345-5787

License No. 0504035

COMPLIANCE

OSHA Pulls the Plug on Electronic Reporting Rules

FEDERAL OSHA has suspended its much anticipated and dreaded electronic filing rules for workplace injury and illness records.

The rules, put in place during the Obama administration, would have required organizations with 250 or more employees to submit electronically information from OSHA Forms 300 (Log of Work-Related Injuries and Illnesses), 300A (Summary of Work-Related Injuries and Illnesses), and 301 (Injury and Illness Incident Report).

The same rules would also apply to employers with between 20 and 249 employees in certain industries, including agriculture, construction, manufacturing, retail and transportation.

A major thrust of the rules was to name and shame employers with poor workplace safety histories, and the latest move will essentially keep these records from being published.

The requirement was to be phased in over two years. This year, all covered establishments had until July 1 to turn in their 2016 forms electronically, but OSHA never launched the website for companies to submit the information.

The employer community, particularly the construction industry, had heavily lobbied the Trump administration to jettison the new rules, saying that if injury records were publicized they could unfairly hurt the reputation of employers.

The new rules were supposed to be an extension of an OSHA requirement between 1995 and 2012 that required some 180,000 establishments in high-hazard industries to submit their 300A forms by mail. The program lapsed in anticipation of the now extinguished new rules.

Then in May, OSHA wrote on its website that it "is not accepting electronic submissions of injury and illness logs at this time, and intends to propose extending the July 1, 2017 date by which certain employers are required to submit the information."

As a result, the existing rules for the forms remain in place – and particularly that employers post Form 300A in a conspicuous place in the workplace every year starting Feb. 1 for three months.

While employers are not required to send their completed forms to OSHA, they must retain the forms at their establishments for five years after the reference year of the records. ❖

Complying with Existing Regs

Even if you are not focused on qualifying for either of these exemptions, there are still other important things to remember about posting your 300A:

- If you are required to post a 300A, you need to do so whether or not you had any injuries in the past year. It is completely appropriate – and *required* for covered businesses – to post a 300A saying that you had no injuries or illnesses.
- Sign the 300A when you post it. That is required, and something businesses often forget to do.
- Post the 300A in an accessible location where employees can easily see it, and keep it posted until April 30.
- Be sure to post the 300A, and *not the 300*. Not only is this problematic because it is the incorrect form, but the 300 contains employee names, so making it public can result in privacy violations.
- You do *not* need to post the official 300A form from OSHA's website; it is acceptable to post your own, homemade form containing equivalent information if you would prefer to do so.

Continued from page 1

Address Every Aspect of Your Operation with Management

Take a holistic approach

Every facet of your operation needs to be addressed if you want a comprehensive risk management culture to exist.

Extend discussions about risk management beyond the worksite to help managers see the bigger picture of why safety matters.

Assessing risks associated with every task, purchase order, estimate or piece of equipment used will reinforce the notion that risk management is a company-wide function.

Make periodic site visits

Leadership should visit departments to watch workflows and reinforce the importance of safety to the workers. Make the visits with the manager who has been put in charge of safety for that department.

Leadership's role should be to start conversations with workers about safety challenges and asking for ideas for improving safety.

Use these visits to celebrate successes and challenge the team to always look for issues that could lead to injuries. ❖

EMPLOYMENT PRACTICES LIABILITY

Preventing the Many Forms of Workplace Bullying

ONE WAY TO risk an employee lawsuit is workplace bullying, if you don't investigate when you learn about it and nip it in the bud if you find it's going on.

Old-school cajoling and demeaning employees can these days land a company in hot water and at the receiving end of a costly lawsuit. The problem that many employers face when confronted with bullying is that it's not always cut and dried and there are different types of bullying, some more or less overt than others.

And you also have to decide where the boundary is between harsh words or rude behavior, and bullying. Bullying can be verbal or non-verbal, and it can be overt or someone can be bullied behind their back through rumors and actions that mask the identity of the perpetrator.

To create a bullying-free workplace you need prevention rules in place. But in order to prevent it, you should first understand how it manifests itself. The article "The Dimensions of Workplace Bullying Behavior" by Edward Stern in EHS Today outlines it this way:

OVERT BULLYING

- Refusing to talk to someone or meet with them, or sidelining them from meetings they should be in.
- Shouting or cursing at someone either privately or publicly.
- Public humiliation.
- Physical intimidation like gestures or expressions, standing too close to someone and invading their space or blocking someone from entering or leaving an area.

HIDDEN BULLYING

Someone being bullied may not even know it until they learn about it from somebody else. It's done behind their back to undermine them and put their job at risk. It includes:

- Spreading rumors or gossip about a person to hurt their reputation. Gossip, true or not, is a malicious act.
- Not informing someone about meetings that they would normally be included in.
- Purposefully withholding vital information from the worker when they need to know it to do their job.

BULLYING ONLY BOSSES CAN DO

There are some forms of bullying that can only be done by supervisors or managers to undermine or disgrace an employee, like:

- Setting impossible deadlines.
- Removing responsibilities without cause.
- Frequently changing work guidelines.
- Cancelling an employee's vacation.
- Underworking someone so they feel useless.

What's not bullying

Not all moments when a worker is feeling uncomfortable due to the actions of another employee or supervisor are bullying, like:

- A civil disagreement or argument.
- Factual, civil, professional criticism of work by a supervisor.
- Bad management decisions that were not intended to degrade or undermine a worker.
- Not greeting someone when they arrive at work.

Setting the rules

Fold your anti-bullying rules in with the rules you have in place for prevention of discrimination and harassment. They should:

- Define bullying so that both employees and management can easily identify the behavior and address it.
- Make it clear that victims should not be fearful of losing their jobs or risk retaliation should they report bullying.
- Set up a system for employees to report bullying or use the same mechanisms you have in place for reporting discrimination or harassment.
- Require management to respond quickly to reports of bullying. They should conduct an investigation immediately and, even if names are not provided, the organization needs to let others in the company know when it has taken action – and what the consequences were.

One big danger is to ignore bullying because you think it adds to productivity or profitability. That's a big mistake.

Your organization should have a zero-tolerance attitude around bullying – no matter who the bully is, or how high up they are in your hierarchy. ❖

Risk Management

Staff Texting Blows Holes in Communications Policies

YOU MAY not be aware of it, but your employees are most likely communicating with each other and clients using texting or instant messaging.

While the immediacy of texting and instant messaging is great for business as it allows faster communications, better collaboration and more responsiveness, the downside is that your organization likely can't track and retrieve those communications.

It becomes even harder if the communications are via instant messaging apps like Whatsapp and Facebook's Messenger.

As an employer, it's important that you understand the issue and that you have clear rules for communications among employees in order to protect your company's interests.

You'll need a policy in place when something goes wrong and you need to track the thread of communications to see what was said or promised by whom, and when. These details can be crucial to resolving problems with clients, or if you are ever sued and your communications are subpoenaed for discovery.

Plaintiff-side lawyers in employment cases have already started demanding the production of text messages and e-mails during discovery. And if litigation ensues on an issue, you may have a duty to preserve text messages.

Roadblocks

There are a few issues that you need to consider, especially in light of the fact that many companies are allowing staff to use their own devices for company communications, including giving them access to the business's e-mail system on their phone.

If your employees are exchanging texts and instant messages on company phones, the history of communications would be preserved and you would be able to access the content by asking for the phone.

But, if your employees are sending and receiving work texts and instant messages on their personal devices, the issue gets murkier, particularly if you don't have a bring-your-own-device (BYOD) policy. Accessing messages about company business on an employee's smartphone may raise privacy issues.

The problem especially arises in the case of wrongdoing by an employee. If they are using their phones for communications that could provide insight into their behavior, they can erase those messages before you ask to see them.

In other words, you cannot rifle through their phone without first obtaining it, meaning you can't look at it without them knowing as you could if you looked at their e-mail on your company server.

There are also privacy issues that arise if you are trying to access an employee's personal phone to view texts and messages.

The big issue is: how do you capture those communications? After all, it will not be done over your network, unlike your company's e-mail system that preserves all communications which are available to you. The messages reside on the phone instead.

What you should do

Obviously texting and instant messaging are a potential minefield for employers who want to be able to access all company communications among employees and between your staff and clients, vendors or partner organizations.

To ensure you have a handle on it, you should set rules outlining what method of communication employees may use for business purposes.

If you don't want texting or instant messaging of any kind for company business, that needs to be spelled out – including ramifications for breaking the rule.

If you decide to allow texting and instant messaging, your policy should be clear on what kind of communications are okay.

You will need to amend your policy related to employee communications and record retention to make sure texts and instant messages are included.

If you have a BYOD policy, at a minimum it should include allowing you to take custody of the employee's phone for legitimate purposes like a dispute with a client, or discovery for litigation.

As you can see, it's important that you initiate a policy on employee communications that takes into account texting and messaging.

If you haven't done so, you should do it now as this faster method of communication is becoming the new normal, particularly as Generation Y continues filtering into the workforce. ❖