



Account Managers

Leslye D'Amico
Jill Porter

HR Consultants

Scott Andreassen
Dan Baltzer

HR Representatives

Rick Mathisen
Jeanne Obert

Payroll Specialists

Nan Foster
Mike Tecca

Benefits Specialists

Greg Natyshak
Michelle Hayes

Operations Specialist

Murriel Watson

Retirement Plan Specialist

Katie Peters

Risk Manager

Jonathan Hall

Accounting

Nancy Storms

Receptionist

Mary Budzak

Administrative Assistant

Nou Vang

Executive Assistant

Lori Goold

Director of Sales & Marketing

Terri Swanson

VP of Finance & Compliance

Dan Fouberg

VP of Operations

Jodi Goda

VP of HR & Client Services

Carol Gilson

President & CEO

Alan Reid



**Insight Into HR News With EMPO
1st Quarter Edition 2007**

In This Issue You'll Find:

- **Upcoming EMPO Events**
- **OSHA Recordkeeping**
- **Business Continuity Planning**

Is there a subject that you would like to know more about in a future newsletter? Please feel free to send me an email and let me know at lgoold@empocorp.com.

MARK YOUR CALENDARS 2007 Client Educational Breakfast Seminars

Three complimentary seminars for business owners, managers and/or supervisory personnel are scheduled for 2007. Based on feedback we've received from attendees at our 2006 seminars, the following topics will be featured at our 2007 seminars. Although you will receive a special invitation noting the location for each seminar, please mark your calendars for these events.

March 15, 8–10:30 a.m. Performance Management

Managing performance of employees begins at the offer letter stage of employment and ends at termination of employment. It includes creating expectations, setting goals plus giving feedback and rewards (if appropriate). This will enable employees to understand what's expected of them, so they can have a successful employment relationship and add value to your organization.

June 7, 8–10:30 a.m. Preparing & Conducting Performance Reviews (for both excellent and wayward employees)

Performance reviews are only one part—but a critical part—of an entire Performance Management System. Whether an organization has a formal or informal system, there's a significant difference in how a manager prepares and conducts reviews for either of these employees to achieve the desired results.

September 20, 8–10:30 a.m. Effective Communications & Conflict Resolution

Whenever people are working together, it is a fact that conflict will occur. If, however, communications are effective it will minimize conflict. How conflict is handled and resolved can be critical to the success of the employee and to the working relationship with supervisors and coworkers.

By attending these seminars you will learn many practical ideas that EMPO's HR professionals have found that result in employee retention and satisfaction. Applying these practices will improve supervisors' effectiveness, employees' success on the job and ultimately our organizations' success.

Also, if you wish to have others in your organization added to our electronic mailing list, please let us know so that they can be included in future communications and invitations.

*One of your purposes
in life should be to
draw out your own
innate capabilities as
well as the capabilities
of those around you.*

—Anonymous

*When you have to
make a choice and
don't make it, that is
in itself a choice.*

—William James

*To eliminate a
problem, you must get
to the root of it.
Unless you do that, it
will sprout again.*

—Anonymous

*The circumstances of
others seem good to
us, while ours seem
good to others.*

—Publilius Syrus



Coming Soon...

2006 OSHA FORM 300A Annual Summaries

In mid-January, EMPO Corporation's Risk Management Department will send your 2006 OSHA Form 300A Annual Summaries. This will be sent to your main office. Please have an executive of your company sign the Form 300A and post it from February 1, 2007 until April 30, 2007 (if applicable). According to OSHA's recordkeeping rules, some industries are exempt from OSHA recordkeeping. In those cases, your company will receive a summary, but it will be for your records only and will not need to be posted. Check the detail page that will accompany your form for your specific posting requirements.

Please note...

When an injury occurs, it is not always immediately known whether it is recordable. It may take review of medical dictation to make this determination. If an injury is determined not to be recordable by OSHA standards, then it will not show up on your OSHA 300 log or Form 300A Annual Summary.

If you have any questions, please contact Risk Manager Jonathan Hall at (612) 285-6215.

Business Continuity Planning

Three-of-three in a Series on the Business Continuity Planning Process

The third and final stage of business continuity planning involves more support to your employees' well being, while reviewing key processes and protecting your physical assets as well.

Support Employee Health After a Disaster

1. Encourage adequate food, rest and recreation.
2. Provide for time at home to care for family needs, if necessary.
3. Have an open door policy that facilitates seeking care when needed.
4. Create opportunities for breaks where co-workers can talk openly about their fears and hopes. Sharing with others can speed personal recovery.
5. Reassure your employees that families will be supported. This will help alleviate their worries, which can consume an employee—especially one who may have experienced a disaster.
6. Re-establish routines when possible. Workplace routines facilitate recovery by providing an opportunity to be active and to restore social contacts.
7. Offer professional counselors to help co-workers address their fears and anxieties.
8. Once the need to listen for emergency instructions has passed, limit television, radio and other external stresses.
9. Take care of yourself. Leaders tend to experience added stress after a disaster. Your personal health and recovery is important to your family and your employees.

Review Insurance Coverage

1. Meet with your insurance provider to review current insurance coverage for such things as physical losses, flood coverage and business interruption.
2. Understand what it covers and what it does not.
3. Understand what your deductible is, if applicable.
4. Consider how you will pay creditors and employees.
5. Plan how you will provide for your own income if your business is interrupted.
6. Find out what records your insurance provider will want to see after an emergency and store them in a safe off-site place.



Business Continuity Planning (Cont.)

*Do the job so well that
even your toughest
critic—YOU—can take
pride in the results.*

—Anonymous

*Get control over your
emotions—know when to
summon empathy and
how to be tolerant when
you must.*

—Anonymous

Trust your gut.

—Barbara Walters

*Think big. At the same
time, be able to be aware
of the smallest details.*

—Anonymous

*It is tact that is golden,
not silence.*

—Samuel Butler

Prepare for Utility Disruptions

1. Plan ahead for extended disruptions during and after a disaster. Carefully examine which utilities are vital to your business' day-to-day operations. Speak with service providers about potential alternatives and identify backup options, if applicable.
2. Learn how and when to turn off utilities. If you turn the gas off, a professional must turn it back on. Do not attempt to restore the gas yourself.
3. Consider purchasing portable generators to power the vital aspects of your business in an emergency. Never use a generator inside as it may produce deadly carbon monoxide gas. It is a good idea to pre-wire the generator to the most important needs. Periodically test the backup system's operability.
4. Decide how you will communicate with employees, customers, suppliers and others. Use cell phones, walkie-talkies, or other devices that do not rely on electricity as a backup to your telecommunications system.
5. Plan a secondary means of accessing the Internet if it is vital to your company's day-to-day operations.
6. If food storage or refrigeration is an issue for your business, identify a vendor in advance who sells dry ice in case you can't use refrigeration equipment.

Secure Facilities, Buildings and Plants

1. Install fire extinguishers and smoke detectors in appropriate places.
2. Locate and make available building and site maps with critical utility and emergency routes clearly marked.
 - Plan to provide a copy to local firefighters or other first responders in the event of a disaster.
 - Keep copies of these plan documents with your emergency plan and other important documents in your emergency supply kit.
3. Consider if you could benefit from automatic fire sprinklers, alarm systems, closed circuit TV, access control, security guards, or other security systems.
4. Secure ingress and egress. Consider all the ways in which people, products, supplies and other things get into and leave your building or facility.
5. Identify what production machines, computers, custom parts or other essential equipment is needed to keep the business open.
 - Plan how to replace or repair vital equipment if it is damaged or destroyed.
 - Identify more than one supplier who can replace or repair your equipment.
6. Store extra supplies, materials and equipment for use in an emergency.
7. Plan what you will do if your building, plant, or store is not usable.
 - Consider if you can run the business from a different location or from your home.
 - Develop relationships with other companies to use their facilities in case a disaster makes your location unusable.
8. Identify and comply with all local, state, and federal codes and other safety regulations that apply to your business.
9. Talk to your insurance provider about what impact any of these steps may have on your policy.

Protect Mail: Safety Tips

1. Teach employees to be able to quickly identify suspect packages and letters. Warning signs include:
 - Misspelled words
 - No return address
 - Excessive use of tape
 - Strange discoloration or odor
2. The United States Postal Service suggests that if a suspect letter or package is identified:
 - Don't open, smell, touch or taste
 - Immediately isolate suspect packages and letters
 - Move out of the area
 - Quickly wash with soap and water and remove contaminated clothing
 - Contact local law enforcement authorities

Business Continuity Planning (Cont.)

Secure Your Equipment

1. Conduct a room-by-room walk-through to determine what needs to be secured.
2. Attach equipment and cabinets to walls or other stable equipment.
3. Place heavy or breakable objects on lower shelves.
4. Move workstations away from large windows, if possible.
5. Elevate equipment off the floor to avoid electrical hazards in the event of flooding.

Assess Building Air Protection

1. Know the Heating, Ventilation, and Air-Conditioning (HVAC) system.
 - Building owners or managers, and employees should take a close look at the site's system and be sure it is working properly and is well maintained.
 - Be sure any security measures do not adversely impact air-quality or fire safety.
2. Develop and practice shut-down procedures for the HVAC system.
3. Secure outdoor air intakes. HVAC systems can be an entry point and means of distributing biological, chemical, and radiological threats.
 - Limit access to air intake locations to protect people inside a building from airborne threats. Air intakes at or below ground level are most vulnerable because anyone can gain easy access.
 - Consider relocating or extending an exposed air intake, but do not permanently seal it.
4. Determine if you should feasibly upgrade the building's filtration system.
 - Increasing filter efficiency is one of the few things that can be done in advance to consistently protect people inside a building from biological and some other airborne threats.
 - Carefully consider the highest filtration efficiency that will work with a building's HVAC system.

Protect and Improve Cyber Security

1. Use anti-virus software and keep it up-to-date.
 - Activate the software's auto-update feature to ensure your cyber security is always up-to-date. Think of it as a regular flu shot for your computer to stop viruses in their tracks.
2. Don't open email from unknown sources.
 - Be suspicious of unexpected emails that include attachments whether they are from a known source or not.
 - When in doubt, delete the file and the attachment, and then empty your computer's deleted items file.
3. Use hard-to-guess passwords.
 - Passwords should have at least 8 characters with a mixture of uppercase and lowercase letters as well as numbers.
 - Change passwords frequently.
 - Do not give your password to anyone.
4. Protect your computer from Internet intruders by using firewalls.
 - There are two forms of firewalls: software firewalls that run on your personal computer, and hardware firewalls that protect computer networks or groups of computers.
 - Firewalls keep out unwanted or dangerous traffic while allowing acceptable data to reach your computer.
 - Don't share access to your computers with strangers.
 - Check your computer operating system to see if it allows others to access your hard-drive. Hard-drive access can open up your computer to infection.
 - Unless you really need the ability to share files, your best bet is to do away with it.

*The only difference
between success and
failure is the ability to
take action.*

—Alexander Graham Bell

*An error gracefully
acknowledged is a victory
won.*

—Caroline L. Gascoigne

EMPO Corporation

3100 West Lake Street
Suite 100
Minneapolis, MN
55416

Phone

612-285-8707

Fax

612-285-8708

e-mail

lgould@empocorp.com

www.empocorp.com

By Rick Mathisen, HR Representative

