

Marshall & Sterling

INSURANCE

Leeds ♦ Saratoga Springs

*Our People Are Your
Best Insurance*

*Lorraine Emerick, VP
January 2017*

January



In this issue:

OSHA's electronic reporting rule, the FAA's oversight of commercial drone use and a new FMCSA database for drug and alcohol testing.

Predictions for cyber attacks in 2017, a new malware campaign that affects over 1 million Google accounts and the recent shutdown of a cyber crime ring.

How to keep your resolutions throughout the year, space heater safety and what to look for when buying a used vehicle.

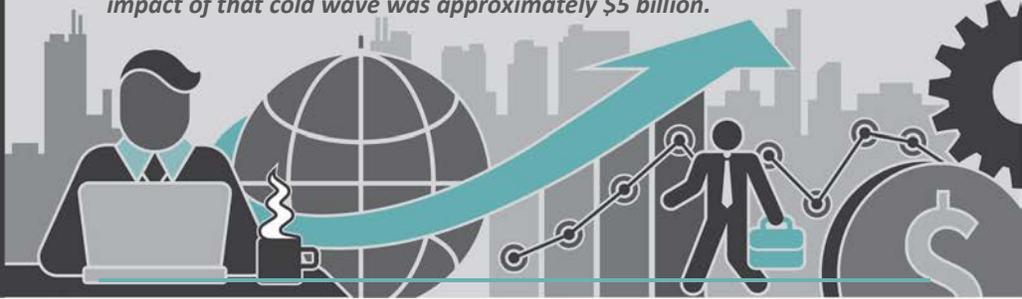
Proud Supporter of the Business Incubator Assoc. of NYS

JAN 2017

P&C PROFILE

DID YOU KNOW?

Meteorologists believe that a polar vortex—a low pressure system that causes rapid temperature drops—is to blame for colder-than-normal temperatures in the United States this winter. Polar vortices also contributed to a cold wave in the winter between 2013 and 2014, and weather intelligence firm Planalytics estimates that the economic impact of that cold wave was approximately \$5 billion.



IN THIS ISSUE

- **OSHA's Electronic Reporting Rule.** A new rule from the agency becomes effective on Jan. 1, 2017, and will require some employers to submit injury and illness data electronically.
- **FAA Criticized for Ineffective Drone Oversight.** An audit conducted by the Office of Inspector General has shown that the FAA has not adequately trained its safety inspectors to enforce commercial drone regulations.
- **New FMCSA Rule Creates Database for Drug and Alcohol Testing.** A new rule will require motor carrier employers to check a database to see whether their current and prospective employees have unresolved violations under the FMCSA's drug and alcohol testing program.

Provided by:

Marshall & Sterling Insurance

[Lorraine Emerick, VP](#)

**Marshall
& Sterling**

INSURANCE

LEEDS ♦ SARATOGA SPRINGS

www.marshallsterling.com/leeds

OSHA's Electronic Reporting Rule

OSHA currently requires employers to keep track of their employees' injuries and illnesses in an "OSHA log." However, in 2016, the agency released a final rule that will also require some employers to submit these records electronically, so they can be posted on OSHA's website. The final rule becomes effective on Jan. 1, 2017.

The following are the requirements for the new rule:

- Establishments with 250 or more employees that are required to keep injury and illness records must electronically submit the following forms:
 - OSHA Form 300: Log of Work-Related Injuries and Illnesses
 - OSHA Form 300A: Summary of Work-Related Injuries and Illnesses
 - OSHA Form 301: Injury and Illnesses Incident Report
- Establishments with 20-249 employees that work in industries with historically high rates of occupational injuries and illnesses must electronically submit information from OSHA Form 300A.

With the new rule, OSHA hopes that employers and researchers will be encouraged to find new and innovative ways to prevent injuries and illnesses at workplaces.

For more information on the recordkeeping rule, contact us at 800-724-0695. We can provide you with our in-depth compliance bulletin, "OSHA Issues Final Rule on Electronic Reporting."

FAA Criticized For Ineffective Drone Oversight

According to a [report](#) released by the Office of Inspector General, the Federal Aviation Administration (FAA) has mishandled a large number of safety violations regarding the use of unmanned aerial systems (UASs), commonly referred to as drones.

Since the FAA has authorized the use of drones for commercial purposes, the agency has granted more than 5,500 exemptions to businesses to allow for the use of drones. However, the report states that the FAA has not responded to the increase in drone operators by adequately training its staff about the new rules for commercial drones. In many instances, the agency also failed to respond to reports of safety violations—at times taking months to respond to complaints.

In addition to a lack of training for inspectors, the report also stated that the FAA lacks a robust data reporting and tracking system for drone activity, and that any available information is difficult to analyze as a result of fragmentation.

For more information on the current rules regarding the commercial use of drones, contact Marshall & Sterling Insurance today.

[Lorraine Emerick, VP](#)

New FMCSA Rule Creates Database for Drug and Alcohol Testing

The Federal Motor Carrier Safety Administration (FMCSA) recently released a final rule that will create a national drug and alcohol testing clearinghouse for commercial driver license (CDL) holders who operate commercial motor vehicles (CMVs). Under the rule, drivers will be added to the clearinghouse if they test positive for drugs or refuse to perform a test required by the Department of Transportation (DOT). Then, employers will be able to review the testing history of applicants, drivers who work for more than one motor carrier and long-term employees.

Once the clearinghouse has been created, employers will be required to do the following:

- Search the clearinghouse at least once every year for current drivers.
- Review the system for any information on driver applicants.

The agency has stated that the rule will assist employers in determining whether a driver needs to begin or continue a return-to-service process before driving a CMV. And, although the final rule becomes effective on Jan. 4, 2017, compliance with it will not be required until Jan. 6, 2020.

For more information on the final rule, call us today and ask to see our compliance bulletin, “FMCSA Creates National Clearinghouse for Drug and Alcohol Testing.”

Study Shows that Employees with Little Flexibility Are Unhealthier

According to research from the Indiana University Kelley School of Business, employees that work high-stress jobs and have little control over their workflow die at a younger age and are generally healthier than their counterparts who have more flexibility.

Although the report does not suggest that employers cut back on the amount of work that they give to employees, experts believe that a larger amount of flexibility could help employees be more productive and healthier overall.

CYBER RISKS+LIABILITIES

[Visit our Cyber Center](#)

IN THIS ISSUE

Report Predicts Escalation of Cyber Attacks in 2017

A new report makes five major predictions about how cyber attacks will escalate in number and severity in 2017.

New Malware Campaign Affects 1 Million Google Accounts

A malware campaign downloads unauthorized apps onto a user's device in order to generate advertisement revenue.

Authorities Shut Down Cyber Crime Ring

A large group of hackers called the Avalanche network has been shut down by authorities in the United States and the European Union (EU).



**Marshall
& Sterling**

INSURANCE

LEEDS ♦ SARATOGA SPRINGS
www.marshallsterling.com/leeds

Report Predicts Escalation of Cyber Attacks in 2017

According to a recent report from Experian, a global information services group, businesses can expect to see an increase in the number and severity of cyber attacks in 2017. The report also predicts that a large number of politically-motivated cyber attacks near the end of 2016 will escalate into a larger cyber attack conflict, and that businesses in the financial, security and health care industries will be the most frequently targeted.

Major Predictions

As a part of the report, Experian made five major predictions for cyber attacks in 2017:

- Password breaches will contribute to the abandonment of the password as a security measure. Although the theft of login IDs and passwords constitutes a short-term threat, the report states that cyber criminals continue to sell passwords long after they are stolen. And, as businesses and consumers are lured into a false sense of security after their password is unknowingly stolen, passwords alone will begin to fall out of favor. Instead, the report emphasizes that two-factor identification—where two separate pieces of authentication evidence are required—should be used by businesses to defend against cyber attacks.
- New, sophisticated attacks will continue to target the health care industry. Because medical identities and information remains relatively easy to access and profitable for hackers, the health care industry will continue to be a target in 2017. The report also states that large establishments, such as hospital networks, will continue to face threats like ransomware, a type of attack where an organization is “locked out” until a financial ransom is paid.

(Continued on next page)



Research Shows that Overcompensation for Cyber Attacks Can Backfire

Research conducted by the Sam M. Walton College of Business and the Billingsley Chair of Information Systems has shown that consumers are often suspicious when they are given too much compensation following a cyber attack.

The research noted that because it can be difficult to ascertain the exact costs of a cyber attack, offering appropriate compensation to consumers can be just as challenging.

For example, in 2013, a cyber attack against Target affected 110 million customers. After the attack had been resolved, Target offered customers a 10 percent discount on purchases—an offer that was met favorably. However, the research found that customers grew suspicious when the company also offered free credit monitoring as reimbursement.

Authorities Shut Down Cyber Crime Ring

Authorities in the United States and EU recently shut down a network of hackers known as the Avalanche network. The group had operated since at least 2010 and targeted more than 500,000 computers with a variety of cyber attacks.

The Avalanche network was also used as a platform to distribute and purchase malware for a variety of purposes—though the network was mostly used to steal online banking information or to install ransomware on various computer systems.

It was recently revealed that a state prosecutor's office in Pennsylvania was targeted by one of the Avalanche network's ransomware attacks and was forced to pay \$1,400 in bitcoin to release its infected computer network. However, it's unknown if the cyber crime ring targeted additional government agencies. Five known members of the group are currently facing charges in numerous countries.

(Continued from previous page)

- **Politically-motivated and state-sponsored attacks will become more common.** The large number of high-profile cyber attacks at the end of 2016, along with the accusation that many of the attacks were state-sponsored, may lead to businesses being affected by the collateral damage of these attacks. Additionally, the report predicts that such attacks will only grow as politically-motivated hackers seek retaliation against others.
- **Hackers will focus on payment-based attacks, despite new credit card security measures.** Although the switch to EMV chip cards and the PIN liability shift were expected to protect against payment breaches, uneven adoption could lead to additional cyber exposures in 2017. Additionally, criminals are beginning to use sophisticated skimming machines to steal card data at physical retail and ATM locations.
- **International data breaches will cause major problems for multinational businesses.** The loss of consumers' data is a large problem if it occurs in just one country, but multinational businesses must also deal with ever-changing regulations in all of their markets. The United States, EU, Australia and Canada have all passed new regulations that will force businesses to re-evaluate their cyber security plans.

New Malware Campaign Affects 1 Million Google Accounts

A malware campaign called Googlian has breached over 1 million Android devices, and continues to affect approximately 13,000 devices every day. The malware is capable of stealing a user's authentication, which allows it to gain access to personal data from Google Play, Gmail, Google Photos and other platforms.

Googlian uses a Trojan horse attack, in which the malware poses as a legitimate app that is downloaded onto a user's device. However, Googlian uses the data on a user's phone effectively as a marketing scheme, and surreptitiously downloads additional apps onto the device. And, although Googlian has not yet targeted personal information for profit, advertisements located in the apps generate revenue for the hackers.

Google has stated that the Googlian apps come from third-party app stores, and not the company's official Google Play store. As a result, Android users should delete any third-party apps from their devices and only download apps from the official store.

Marshall & Sterling Insurance

300 Route 23B

Leeds, NY 12451

800-724-0695

www.marshallsterling.com/leeds

Lorraine Emerick, VP

inSIGHTS

JANUARY 2017

IN THIS ISSUE

MAKING RESOLUTIONS LAST FOR THE ENTIRE YEAR:

Make sure that your resolutions last until 2018 with these simple tips.

USING SPACE HEATERS SAFELY:

Protect your home from fire hazards by using space heaters safely.

WHAT TO LOOK FOR WHEN BUYING A USED VEHICLE:

Keep these tips in mind before you make a purchase to ensure that a used vehicle is safe and in good condition.

PROVIDED BY

[Marshall & Sterling Insurance](#)

800-724-0695

**Marshall
& Sterling**

INSURANCE

LEEDS ♦ SARATOGA SPRINGS
www.marshallsterling.com/leeds

LIFE

Making Resolutions Last for the Entire Year

The new year usually comes along with new resolutions—spending less, being more active and so on. However, keeping a new resolution a few months down the road can take some serious dedication. Here are a few tips to ensure that your resolutions will last all the way until 2018:

- **Don't set a goal for the whole year.** Although it can be tempting to set a numerical-based resolution for the entire year—such as losing a certain amount of weight or saving a certain amount of money—it can be just as easy to push these goals off until it's too late. Instead, try to focus on what you can do on a regular basis.
- **Be specific.** Generic goals can be much easier to ignore. While a goal like “exercising more” may seem like a good idea, it's easier to follow through if you're specific. Make a schedule for when, where and how you'll accomplish a specific goal.
- **Only do one step at a time.** Resolutions are meant to last for the entire year, not just for a week or a month. Don't try to overexert yourself early in the year by doing too much too quickly—instead be sure to stay consistent and take your resolutions one step at a time.
- **Find a partner.** Doing resolutions with a friend or family member can help you stick to your schedule. Plus, a little friendly competition can help you stay motivated!
- **Know when to take a break.** Although it's important to stay regular with your resolutions, remember that it's OK to take a break every now and then. That way, you'll be able to come back to your goals with a relaxed and refreshed mindset.

HOME

Using Space Heaters Safely

Although space heaters are a great way to warm your home during the cold winter months, they can also present serious home fire hazards. According to the National Fire Protection Association (NFPA), space heaters are involved in 79 percent of fatal home heating fires.

To ensure that your home is both safe and warm this winter, keep these space heater safety tips in mind:

- Only purchase space heaters that have a mark from a reputable certification agency, such as Underwriters Laboratories (UL).
- Check for safety features when you're purchasing a heater—such as an automatic shutoff and heating element guards.
- Check your space heater's cords before you use it to ensure that it doesn't cause an electrical fire.
- Never use space heaters to warm bedding, or place them near any flammable materials.
- Turn off space heaters whenever you leave the room or go to sleep.
- Pay extra attention to children and pets when they're around space heaters.
- Don't place heaters in congested or high-traffic areas of your home. Additionally, make sure that cords don't present a tripping hazard.

AUTO

What to Look for When Buying a Used Vehicle

Buying a used vehicle can be a great and inexpensive way to get on the road. However, you need to be extra careful when buying a used vehicle to ensure that it's safe and in good condition.

Here are some things you should always check before you buy a used vehicle:

- Look for any wear or scratches around the vehicle's dashboard. This could be a sign that the odometer has been tampered with.
- View the vehicle from all angles—including from the ground—to check for wear and tear.
- Check for a damp or moldy smell in the vehicle's interior. This could be a sign of water damage.
- Take the vehicle on a test drive to see how well it performs. Also, pay attention to any clanking or grinding noises that could indicate damage.
- Ask a salesperson to see under the vehicle's front hood. Additionally, you should ask if the vehicle has a printed history report, so you can see if it's been in any accidents or had serious maintenance done.



IN THE KNOW

National Radon Action Month

The Environment Protection Agency (EPA) designates every January as National Radon Action Month in order to make everyone aware of the dangers of radon. This colorless and odorless gas is difficult to detect and is the leading cause of lung cancer in nonsmokers.

Although radon can make its way into any environment or building, the largest exposure area is your home. Luckily, there are two common and inexpensive tests you can use to test your home for radon. A short-term test, which stays in your home for two to 90 days, can be a great way to get a quick idea of your home's radon levels. However, if you want to get a better idea of your home's levels, you can also purchase a long-term test.

If you're concerned about radon or other dangerous gases in your home, contact us at 800-724-0695.