# How Technology Is Helping to Reduce Fraud

**Fraud in all U.S. lines of insurance is responsible for approximately $80 billion per year in losses. Several billion dollars of that is workers comp fraud. In the past few years, however, some of those loses have been reduced thanks to technology.**

### Video and Video Surveillance:

Though the use of drones with cameras on board for investigating fraud is rapidly growing, particularly on stakeouts (see below), claims investigators use video in other ways, as this excerpt from a post on the www.trustify.info blog demonstrates:

*"You wouldn't mind if I… you know… videotaped us working out, would you?" I said to Lifter guy. "Just to look at my form and stuff?"*

*"No problem. You gonna put it on YouTube or something?" Lifter Guy responded.*

*"Yeah," I smirked and smiled, "something like that."*

*Little did Lifter Guy know that I was a Private Investigator (P.I.) working undercover to videotape him powerlifting while cheating the workers' compensation system.*

People like attention, so it's not hard to get their permission to film them even in situations where they should be more cautious. A more common use of video is as a surveillance tool.

Nearly one in four business owners now uses video cameras to monitor employees. A recent YouTube video shows actual footage of a Fort Lauderdale woman who hit herself on the head with a sprinkler head after it fell onto her desk. She is startled at first, then quickly picks the sprinkler head up, leans back in her chair and smacks her head with it. She has been convicted of workers comp fraud. https://www.youtube.com/watch?v=A4N4X_9URKk

Video surveillance can also be helpful in identifying fraud in other ways. For example, parking lot cameras could show how a worker limped from their car and into the building shortly before reporting that the injury to their leg just occurred on the job.

**Prescription Monitoring Database:** Almost every state uses a prescription drug monitoring program to control substance abuse. These databases track drug use by patients as well as the dispensing of drugs by prescribers, making it easier to detect patterns of excessive or fraudulent use of opioids and other controlled substances.

**Social Media:** A workers comp recipient was on leave because of a work-related injury. However, he "could not resist playing a contact sport on a local semi-professional sports team," according to *Risk Management Magazine*. Social media and internet searches revealed the worker was listed on the team roster and having a great season

"Head and shoulders above anything else from falsifying an accident or exaggerating an injury, the biggest trend is how social-media monitoring is being used as an investigative tool to understand and predict future activities of these presumably injured people." Steve Cassell, Lake Mary, Florida-based president and CEO of Command Investigations L.L.C. told *Business Insurance* magazine. "People brag; it never stops."

Keep in mind you can't trick people into giving you access to their social accounts, but if access to their accounts is available to the public, information obtained from them can be used to substantiate allegations of fraud.

**Drones:** Private investigator Mike Stanfield of Apex Investigation Group used to stake out a suspected fraudster for weeks. Now he uses technology. He recently sent a remote camera drone to make short flights near the house of someone suspected of fak-

*FRAUD—continued on Page 3*

**Here's your issue of *Managing Risk* from:**

GAINES INSURANCE

2260 LAVA RIDGE COURT
SUITE #101
ROSEVILLE, CA 95661

PRESORTED
FIRST-CLASS MAIL
US POSTAGE
PAID
MEDFORD OR
PERMIT NO 125

<<OPT. ENDORSEMENT LINE>> <<SACK>>
<<FULL NAME>>
<<COMPANY>>
<<PRIMARY ADDRESS>>
<<SECONDARY ADDRESS>>
<<CITY>>, <<STATE>> <<ZIP>>


# Managing Risk

GAINES INSURANCE

Gaines Insurance Agency, Inc.
2260 Lava Ridge Court, Suite #101
Roseville, CA 95661
Office: 916-773-8000
Fax: 916-773-8004
*License Number: 0H64864*

Managing Risk | Winter 2018 | Volume 28 • Number 1


# Next Cyberattack Could Cost as Much as Superstorm Sandy

**A major cyber attach could cost billions of dollars and, unlike extreme weather, comes without warning.**

The total cost of a worldwide cyber-attack could be as high as $53 billion, according to a report issued by Lloyd's of London in July 2017. That's almost as much as the cost of Superstorm Sandy ($50-$70 billion), the second costliest disaster in U.S. history. But worldwide cyberattacks aren't the only risk for small businesses. 43 percent of cyberattacks target small businesses, according to Small Business Trends.

Cyber-attacks can come from anywhere: nation states, terrorists, criminals, activists, external opportunists and company insiders (both intentional and unintentional). Their motivation may be to gain political, military or economic advantage. Where businesses are concerned, though, they steal money or data they can turn into money, such as credit card numbers, health records, personal identification information and tax returns — or they set up a ransom situation that locks the company's access to its data until the ransom is paid.

The National Association of Insurance Commissioners (NAIC) has identified the main cyber risks as:

- Identity theft as a result of security breaches where sensitive information is stolen by a hacker or inadvertently disclosed, including such data as Social Security numbers, credit card numbers, employee identification numbers, drivers' license numbers, birth dates and PIN numbers.
- Business interruption from a hacker shutting down a network.
- Damage to the firm's reputation.
- Costs associated with damage to data records caused by a hacker.
- Theft of valuable digital assets, including customer lists, business trade secrets and other similar electronic business assets.
- Introduction of malware, worms and other malicious computer code.
- Human error leading to inadvertent disclosure of sensitive information, such as an email from an employee to unintended recipients con-

*CYBER—continued on Page 3*

## This Just In…

**There's a disparity in how baby boomers learn and how younger generations including Generation X and millennials learn that affects safety in the workplace.**

**Christina Lincicome of SAIF Corporation, Oregon's state-chartered workers comp insurer, thinks "full classes on safety will become a rarer occurrence because younger generations don't necessarily learn best that way," she told *Business Insurance* magazine.**

**Lincicome points out that since "millennials are highly intuitive…, safety concerns should be relayed showing the best method quickly and decisively. For boomers, you want to include the entire method and build in time for questions."**

**Younger generations also want to know how changes are going to impact the workplace. They need to know the why; they're not satisfied just knowing what to do.**

**"Millennials bring intuitive problem-solving approaches while boomers carry the social and institutional knowledge. These two can create new approaches by leveraging the best in each other. Generation X is generally excellent at project management. They have been referred to as the latchkey generation and understand what it is like to work alone. They excel in productivity and creativity when you give them a charge, a deadline, and leave them alone," said Ms. Lincicome.**

**We saw a cartoon that put the generational disparity this way:**

**Boomer: Tell me quick, I only have five minutes.**

**Millennial: Tell me quick. I only have a few seconds, send me a message on my iPhone.**

# How Changes at EEOC Could Benefit Employers

**President Trump's appointment to the U.S. Equal Employment Opportunity Commission could signal a more cooperative attitude at the agency.**

Now that the EEOC is likely to have a 3-2 Republican majority under nominee Janet Dhillon, its policies are expected to slant in a more pro-employer direction.

Control at the field office level, where much of the litigation against employers has originated, particularly litigation alleging systemic discrimination, is also likely to be more restrained. But that doesn't mean employers should let their guards down either. You'll still want to make sure you have a good employment practices liability insurance policy.

## Obama Administration

Under the Obama administration, the EEOC often attempted "to engage in litigation tactics to force certain outcomes or to force policies," said J. Randall Coffey, a partner with Fisher Phillips L.L.P. in Kansas City, Missouri, to *Business Insurance*.

Under the new administration the EEOC is not expected, for example, to try to push the boundaries of Title VII. In one such case involving a gay skydiver who said he was fired because of his sexual orientation, conflicting amicus briefs were filed with the appellate court. The EEOC contended that Title VII can be interpreted to apply to sexual discrimination, while the U.S. Department of Justice countered that Title VII does not address sexual orientation.

"The EEOC has been very aggressive in searching out cases on the cutting edge" of federal statutes, including those involving transgender issues, said Gerald L. Maatman Jr., a partner with Seyfarth Shaw L.L.P. in Chicago to *Business Insurance*. "I think when the Republican commissioners take their seats and have a majority, that sort of view of the EEOC will be pulled back," he said.

## Sexual Harassment

One area where the agency is not expected to pull back, however, is with regard to sexual harassment. The recent revelations of sexual harassment and other sexual misbehavior by multiple media and political figures makes this issue "too much of a hot potato for them to cut back on that," according to Richard B. Cohen, a partner with FisherBroyles L.L.P. in New York.

People fundamentally agree that sexual harassment is noxious and should not be tolerated. Speakers attending the recent American Bar Association Labor and Employment Law Conference in Washington pointed out that there is still much harassment in the workplace that goes unreported. "Superstars" are often given a pass because of their power and influence. But tolerance for this behavior is fast disappearing. Given the current climate, suits alleging sexual harassment are likely on the rise.

## A More Conciliatory, Cooperative EEOC?

Still, many employment law attorneys feel the tone of the EEOC will be more conciliatory and cooperative, seeking to help employers achieve compliance in a less adversarial and litigious environment. "We will see more outreach to employers for both training and education purposes, as well as trying to resolve the more complex charges before litigation," said Paul C. Evans, a partner with Morgan Lewis & Bockius L.L.P. in Philadelphia.

EEOC Chairperson Nominee Janet Dhillon herself has said that she thinks the commission should spend more time on conciliation to avoid litigation.

## Beware of Activist States

While the EEOC's approach to litigation is expected to be less expansive under the new administration, many experts feel that this may cause some states to become more active.

"HR professionals should never lose sight of the importance of annual compliance training and keep close tabs on statewide compliance regulations since there is enormous activity occurring at the state level," Barry Hartstein, co-chair of the EEO and diversity practice at Littler Mendelson P.C. in Chicago recently told *Human Resource Executive Online*.

For the most part, clients who carry employment practices liability insurance have coverage that is designed to respond to these kinds of EEOC claims. But, experts warn, businesses that operate in states with a more permissive legal environment should operate with greater scrutiny. Insurance companies will be following events closely, too.

Please call us if you have questions about your employment liability insurance or if you would like to get a quote.

***CYBER***—*continued from Page 1*

taining sensitive business information or personal identifying information.
- The cost of credit monitoring services for people impacted by a security breach.
- Lawsuits alleging trademark or copyright infringement.

## Cyber Risk Management

The primary defense against cyber security loss is a well-designed and conscientiously maintained risk management program. The first step in such a program is to identify the firm's vulnerabilities, including systems, procedures, programming and personnel. The next step is to control those vulnerabilities as much as possible. Here is a short, practical checklist:

1. Make sure all company computers have the latest security software, web browsers and operating systems to protect against viruses, malware and other online threats.
2. Turn on automatic software updates, if that's an option. Many updates specifically address known security risks.
3. Scan all new devices, including USB devices, before they are attached to the network.
4. Use a firewall to keep criminals out and sensitive data in.
5. Use spam filters. Spam can carry malicious software and phishing scams, some aimed directly at businesses.
6. Adopt a privacy policy and post it on your website and other online sites. Your policy tells customers what information you collect and how you use it.
7. Know what Personally Identifiable Information (PII) you're storing on your customers, including where you store it, how you use it, who can access it, and how you protect it. Delete any unneeded information.

No matter what firewalls, software and authentication protocols you've installed, your cyber security system is vulnerable if you're not educating your employees on avoiding risky behavior online. The Workplace Security Risk Calculator, available free at https://staysafeonline.org/stay-safe-online/resources/workplace-security-risk-calculator, lets your employees gauge the level of risk their online behaviors pose. You can get more good advice here: https://staysafeonline.org/business-safe-online/implement-a-cybersecurity-plan.

## Cyber Liability Insurance Policies

Even with a cyber security plan in place, your business still needs a fail-safe to protect it against cyber risk.

Currently most standard commercial lines policies do not provide insurance for cyber risks. You need a special cyber liability policy. Due to the lack of actuarial data, however, it's difficult to price. Insurers deal with this by evaluating each risk according its risk management procedures and risk culture. As a result, cyber risk coverages are more customized and, therefore, more costly.

The type and cost of cyber liability coverage offered by insurers is based on the type of business, its size and geographical scope, the number of customers it serves, its web presence, the type of data it collects and stores and other factors, including its risk management and disaster response plan.

Cyber liability policies might include one or more of the following types of coverage, according to the NAIC:

- Liability for security or privacy breaches. This would include loss of confidential information by allowing, or failing to prevent, unauthorized access to computer systems.
- The costs associated with a privacy breach, such as consumer notification, customer support and costs of providing credit monitoring services to affected consumers.
- The costs associated with restoring, updating or replacing business assets stored electronically.
- Business interruption and extra expense related to a security or privacy breach.
- Liability associated with libel, slander, copyright infringement, product disparagement or reputational damage to others when the allegations involve a business website, social media or print media.
- Expenses related to cyber extortion or cyber terrorism.
- Coverage for expenses related to regulatory compliance for billing errors, physician self-referral proceedings and Emergency Medical Treatment and Active Labor Act proceedings.

For more information about cyber security insurance, please contact us.

***FRAUD***—*continued from Page 4*

ing a back injury. Stanfield discovered that the supposedly disabled man was "tossing around 200 pound rocks re-landscaping his property."

"If you are on any property that does not have a privacy fence around it, you are fair game for the drone camera," according to Stanfield.

**Internet of Things:** As we interact more and more with apps and appliances these days, we leave behind time stamped data records of our whereabouts, actions and even our conversations. That information is now being used in investigations. In Arkansas, a court order was issued to Amazon demanding Echo recordings of a suspect in a murder investigation. In Ohio prosecutors will use data from a fraud suspect's pacemaker to attempt to prove he lied in statements to investigators about how he escaped the fire in his home.

Consumer and privacy groups are concerned about how "Big Data" is becoming increasingly intrusive. The courts and legislators are currently trying to strike a balance between privacy and the proper use of data.

We will undoubtedly keep seeing new technologies introduced to help reduce fraud. If you would like to discuss ways technology might help you reduce fraud and other types of losses at your firm, please contact us.