Gilmore Company LLP

2600 Skymark Avenue
Building 9, Suite 201
Mississauga, ON L4W 5B2
Telephone: (905) 602 8009
Facsimile: (905) 602 8011
Toll Free: 1(877) 612 4400
Email: general@gilmoreandco.com

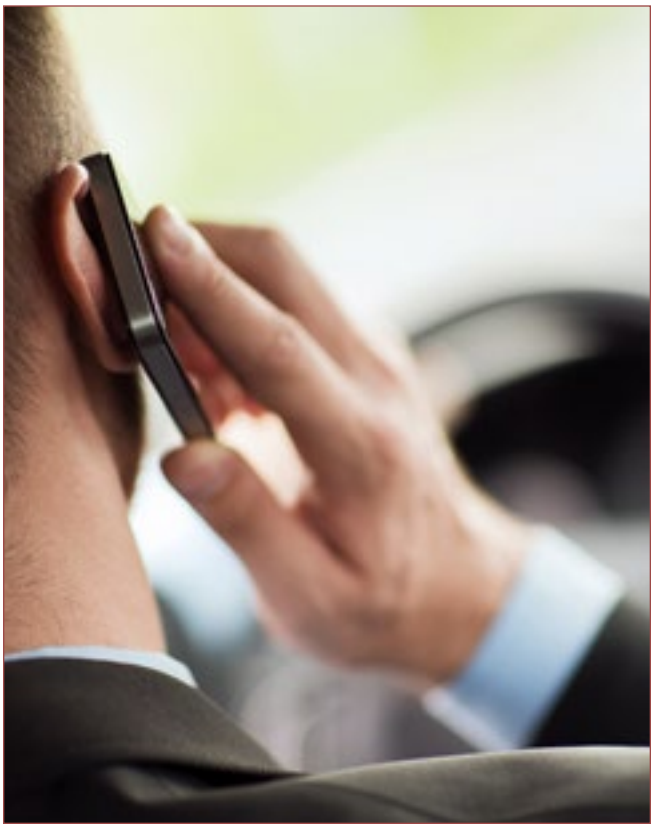
Business Matters

VOLUME 28 | ISSUE 2 | APRIL 2014

MONEYSAVER

The High Cost of Distracted Driving

Employees who drive while distracted create substantial financial and other risks for their employers.



Distracted driving laws are now the norm in all provinces within Canada. Of the three territories, Nunavut is the only holdout. In addition to levying fines, the majority of the provinces and territories have imposed demerit points.

Even with fines and demerit points, many drivers are not convinced that distracted driving affects their ability behind the wheel. A March 3, 2014, news release from the Ontario Provincial Police stated:

> In 2013, distracted driving fatalities surpassed both impaired and speed related fatalities in fatal motor vehicle collisions investigated by the OPP.

A total of 78 people died from distracted driving-related crashes compared to 57 deaths in impaired driving related crashes and 44 people who died in speed related crashes last year.

Both owner-managers and employees should be concerned about these figures, not only because of the unnecessary loss of life, but also because a laissez-faire attitude could ultimately cost owner-managers their business and employees their jobs.

U.S. Lessons

To bring home the point, consider that within the United States, lawsuits have been brought against companies in which it was alleged the company was responsible for employees' actions:

- In Virginia, a law firm settled for an undisclosed amount after a $25-million lawsuit was launched against one of its lawyers for allegedly striking and killing a 15-year-old girl while talking business on a cell phone.
- In Arkansas, a lumber company paid $16.2 million when an employee seriously injured a woman in a vehicular accident.
- In Florida, a company sales person talking on a cell phone seriously injured a 78-year-old woman. The end result was a $21 million settlement.

Although these actions took place in the United States, they demonstrate the need for employers to ensure all personnel are aware of the potential consequences of distracted driving. In Canada, under the legal doctrine of "vicarious liability," an employer may be held legally responsible for negligent acts committed by an employee while the employee is on company business.

Due Diligence

Steps to establish that an employer has exercised due diligence and care include:

- determining the types of electronic devices used by employees in their vehicles
- developing a road safety policy that incorporates guidelines for the use of all hand-held devices
- developing a clearly worded distracted-driving policy for the use of hand-held devices. All employees of the organization should be required to sign off that they have read and understood the policy. A signed copy of the policy should be provided to the employee and one maintained in the employee's file.

In-house seminars should explain the risks of distracted driving.

In-House Awareness

Employers should make attendance at distracted-driving seminars a mandatory condition of employment. The seminars should explain clearly what constitutes distracted driving and its potential impact not only on the business but also on the employees.

Such a seminar should:

1. emphasize that the use of hand-held devices while driving is against the law and that company policy is consistent with the law
2. provide examples of the potential dangers involved in various distracted-driving scenarios
3. direct staff not to accept calls, make calls or text while driving
4. direct staff to pull over to the side of the road to take or make calls or to read and respond to texts
5. instruct staff to have a voicemail message that indicates they are driving and cannot respond to calls at that time
6. ensure staff understand that adjusting a GPS smartphone, MP3 player or other device while driving is distracting
7. ensure staff understand the no-phoning and no-texting policies apply whether they are operating a company vehicle or driving their own vehicle while working
8. ensure employees understand that disciplinary action may be taken if they do not follow company policy
9. ensure that all personally owned hand-held devices have hands-free capability
10. install hands-free capability on all company-owned devices
11. make it clear that employees who work in or travel to other provinces must follow the distracted-driving legislation of that jurisdiction

Other Issues

Staff must understand the impact distracted driving penalties may have on their driving abstract and their ability to work for your company. Demerit points, whether for distracted driving or impaired driving, negatively impact corporate vehicular insurance costs and could potentially lead to lawsuits or the cancella-

tion of policies if individuals with bad driving records are involved in accidents.

Seek Legal Guidance
In that distracted driving infractions are a relatively new area of legislation, employers should have legal counsel review programs, contracts or agreements that address distracted driving and the rights of individuals. For instance, employers may wish to know whether termination policies for distracted driving can be incorporated into employment contracts.

Contact Your Insurance Company
Determine whether vehicular insurance policies and/or third-party insurance policies address distracted driving convictions and the potential impact of fines or convictions on your policy and premiums.

Seize the Initiative
Acceptance that distracted driving is as illegal and hazardous as drunk driving is a critical part of any employer-instituted program to increase awareness of the need for personal, company and third-party safety. In-house policies that demonstrate the responsibility of owner-managers for providing clear-cut practices to all employees will not only confirm corporate stewardship but may save your business from litigation and unnecessary costs.

Get Your Employees to Sign
A good example of a Distracted Driving Policy, which may be useful as a model for your own business, can be found at https://www.osha.gov/distracted-driving/modelpolicies.html. It is advisable to have your policy reviewed by legal counsel before asking your employees to sign.

TAXATION

Zappers

New federal legislation is now in place to punish users of electronic sales suppression software.

The federal government is getting tough with businesses that use electronic sales suppression (ESS) software (commonly called "zappers") to delete or modify point-of-sale (POS) transactions for the purpose of evading taxes. Effective January 1, 2014, zapper users will, of course, not only have to pay the unremitted taxes plus interest but will also face substantial fines and even imprisonment if they manufacture, sell or possess these devices. These sanctions have been introduced through amendments to the *Excise Tax Act* and the *Income Tax Act*.

The Old Days
The old cash register system was fairly simple: it recorded sales in five or six basic categories as well as any applicable taxes and produced a summary for bookkeeping purposes. At the end of the day, the cash in the till was expected to equal the total dollar amount of the sales. If sales were not recorded, it was easy to pocket the funds and no one would be the wiser. This

has always been a concern of retailers since they could never be certain that employees had entered all sales.

Then Along Came POS

The advent of computerized POS systems with bar code scanners and radio-frequency identification (RFID) tags was a blessing for most retailers because the system permitted:

- accurate recording of overall sales as well as the ability to categorize the type of sale
- automatic breakdown of the required HST/GST and PST
- the use of sales data to re-order items as required (i.e., inventory management)
- better security since all individuals using the cash register were required to log on when entering the system
- the reduction of labour-intensive data entry by linking sales transactions directly to the accounting software
- the reduction of cash or inventory theft by employees

The Zapper Facilitates Tax Evasion

The introduction of POS systems made it difficult to skim money from the till because all transactions were recorded within the system. The zapper was developed to falsify the electronic records of a POS system in order to evade paying not only income tax but the various sales taxes. The zapper software program is temporarily introduced into the POS system from a USB flash drive to modify records so that fewer transactions are recorded than have actually been processed. The use of the USB flash drive means the program can be removed from the computer without leaving any trace for the auditor to find.

Tax evasion by using zappers is a worldwide problem.

An International Problem

So extensive is the use of zappers that the Organization for Economic Cooperation and Development (OECD), of which Canada is a member, has been working with member nations to determine the potential loss to economies and develop procedures to reduce the loss to government coffers. The OECD produced a report entitled *Electronic Sales Suppression: A Threat to Tax Revenues* in 2013. (http://www.oecd.org/general/searchresults/?q=electronic%20sales%20suppression) The Canada Revenue Agency has more than 5,000 employees dedicated to finding unreported income and ensuring the appropriate taxes have been remitted.

Voluntary Disclosure

For those taxpayers that may have interfered with their POS, CRA advises that they may wish to consider coming forward with full disclosure now, before any investigation of their business is started. It would be advisable to seek the advice of a tax advisor familiar with the workings of the voluntary disclosure process to ensure that the requirements are met. Expert assistance could reduce or eliminate the penalties or prosecution.

Penalties

The new legislation has created both administrative and criminal penalties. Anyone found in possession of, or using, a zapper will be fined $5,000 for the first infraction; subsequent infractions will bring a $50,000 fine. Any person or company that manufactures, develops or makes a zapper available for use will be fined $10,000 for the first infraction and $100,000 for any subsequent infraction. A summary criminal conviction could bring a fine of not less than $10,000 and not more than $500,000 and/or not more than two years in prison. Conviction by indictment could bring a fine of not less than $50,000 and not more than $1 million and/or imprisonment for not more than five years.

In rare circumstances the vendor may be unaware a zapper is being used on the company's POS system. Penalties will be avoided if the vendor establishes that reasonable prudence was exercised to prevent the use of the zapper (e.g., by having the system examined by an expert).

Zappers Do Not Pay Off

As of January 1, 2014, businesses are on notice that CRA will not tolerate electronic manipulation of POS systems to evade the payment of HST/GST and PST, corporate or personal income taxes. The cost of paying past taxes, penalties, fines and the time and money spent to defend a defenceless position will dwarf the dollars squeezed out of the business by trying to avoid paying the fair share of taxes due.

TECHNOLOGY

Beware of Malicious RATs

A RAT is malware that allows a remote "operator" to control your computer from any location.

The acronym RAT brings shivers to even the most experienced anti-virus programmer. A remote access tool (also referred to as remote administration tool), or RAT for short, is a seemingly innocent type of software used to access and control a computer system remotely. As the description depicts, a RAT is not much different from products such as Windows Remote Desktop, TeamViewer or VNC in that it allows an external third party access to your computer to assist with team collaboration, troubleshooting, and/or repairs. Unlike these useful and legitimate tools, however, the software typically described by the acronym RAT is used for nefarious activity and is associated with those who wish to gain access to and control your computer for personal gain or malicious purposes and, as such, do not seek "permission to come aboard."

The use of RATs to gain access to people's private data and personal lives has gone "mainstream." Notable occurrences are popping up more frequently in the news, such as when Cassidy Wolf, Miss Teen USA 2013, and several other victims were spied upon by a 19-year-old computer science student who took over their computer cameras and purportedly attempted to blackmail the teen with unflattering photos and videos.

A RAT Is Powerful

RAT software is incredibly powerful and can leave your computer, and therefore your data and personal life, vulnerable. Once installed, the third party can, without your knowledge:

- turn your computer on and off remotely at will
- install other software
- turn your computer camera on or off and capture images and sound
- immobilize anti-virus software
- make changes to your computer registry
- use your computer to attack other computers
- access credit card or other confidential data

- steal passwords and account information
- override the keyboard and the mouse
- reformat your hard drive
- access storage drives attached to your computer

A RAT can do anything you can do.

A RAT Can Imitate You

In essence, anything you can do while sitting in front of your computer screen, a hacker with RAT software installed on your computer can also do from any remote location, whether it's down the street from your home or office, or across the globe. Maintaining up-to-date software, operating systems, and anti-virus programs has been the mantra of computer security experts since the first Trojan horses started appearing in a 1986 freeware program called PC-Write. Much like other viruses and Trojan horses, this type of malware can be introduced onto your system when you open attachments in your email, download and install software via P2P (peer to peer) file sharing software, or download files from the Internet. To help keep your system clean and secure and eliminate the risk of inadvertently installing a RAT onto your system, remember to follow these general computer safety guidelines:

- Purchase or download software from reputable software companies.

- Deal with known and well-established computer technicians and support companies in your community.
- Avoid the temptation to click on free software pop-ups or add-ons. Even if it appears harmless, you can never be sure how random freeware might impact other software on your computer.
- Carefully review any email that comes in with an attachment. Ask yourself whether you know the person from whom the email came. Even if you do, it might not be wise to follow a link or download an attachment just for the sake of seeing some cute kitten run across your screen.
- Download and install apps to your smartphone from the app store that has been vetted by your carrier. Avoid any third-party apps that provide links to download software, sounds or images to your phone.
- Always run an anti-virus scan on CDs, DVDs or any external data storage device before copying files or installing software.
- Keep your anti-virus software up to date, and always download and install any updates prior to going online or using external storage devices.
- Do not click on or open pop-ups that indicate they have found weaknesses in your system. Hackers have been known to use this scare tactic as a means of planting viruses within your computer.
- Don't download software or upload personal information unless you have a secure connection (HTTPS).
- Run anti-virus scans on data being transferred from one computer to another, even within your own office. It only takes one infected machine to compromise all your data.

Anti-Virus Software Is Reactive, Not Proactive

It is always important to remember that most anti-virus software is reactive – malware or viruses cannot be detected by your anti-virus software unless there is something to find, which means that by the time it is detected, it might already be too late. To make matters worse, hackers are determined and inventive and are always looking for ways to "beat the system." Recently, hackers have been trying to find and exploit vulnerabilities in frequently used software such as Oracle Java and Adobe Reader. This tactic is devious because these applications are not typically built to protect against such invasions and are not designed with the "beefed up" security of Microsoft Windows and other operating systems.

Be Vigilant

While this new pattern of attack may leave the unsuspecting user at greater risk, a vigilant computer security regimen will help to protect against these hackers and can keep even the RATs at bay.

MANAGEMENT

Put It in the Safe

An office safe is a small investment to make for the security of important documents.

Owner-managers are constantly bombarded with warnings about the need to keep electronic data secure. But what about the old problem of keeping paper documents secure? Indeed, with all the talk about backup, cloud security and off-site storage, it is possible to forget those paper documents and records whose originals must be kept, even if electronic copies have been made. In fact, at the end of each workday, temporary documents, backup drives, cash, negotiable instru-

ments as well as confidential documents need to be secured overnight against theft and fire.

The protection of these objects has a simple, low-tech answer: an office safe. There are all kinds of safes on the market including wall safes, floor safes, gun safes and the small compact utility safes. Most businesses, however, need something larger than a wall safe but without the inconvenience of a floor safe. A stand-alone safe that can be bolted to the floor will suffice for most business purposes.

Types of Safe

Safes come in three main types:

- fire rated
- burglar rated
- composite (i.e., rated for both fire and burglary)

Fire Rated v. Burglar Rated

Safe manufacturers recommend against the use of a fire-rated safe to protect valuables because the walls contain the fire-retardant material and are thus easier to cut or drill than the walls of burglary-rated safes. Don't forget that burglars often take the safe offsite to a place where they have sophisticated tools for cutting and drilling. Composite safes are a very common solution to the risks of both fire and burglary.

The quality and price of a burglary-rated safe should depend on the value and number of objects you plan to keep in it over the next decade or so. As your business grows, you do not want to be trying to fit new, important documents into a small, cheap safe! Talk to your insurance broker about the size and rating of the safe you need for the value of the objects you intend to store.

A fire-rated safe should be able to protect paper and magnetic media from the effects of heat if the office catches fire. Fires burn at about 700°C. Since the ignition temperature of paper is 233°C and CD/DVDs may start to destruct around 345°C, the safe needs to maintain an internal temperature low enough to protect the contents from ignition for at least an hour. The safe should also have smoke seals around the door that expand when heated and thus protect the data stored inside from smoke damage. The thicker the walls and door of the safe, the more insulation used to protect the contents.

Underwriters Laboratories Testing

Manufacturers of quality safes will meet or exceed Underwriters Laboratories or equivalent standards. The usual test has three stages:

1. Fire Endurance

The temperature of the test-furnace fire is brought to 926°C and maintained at that temperature for one hour or raised to 1010°C and maintained for two hours. After this time, the safe is allowed to cool. The inside sensors measure the temperature. To meet the ratings, the temperature cannot exceed 176°C, the temperature at which you would roast a chicken in a home oven. Once the safe has cooled sufficiently, it is examined to determine whether the locking system is still workable.

2. Explosion Hazard

The safe is locked and placed into a furnace heated to 1093°C. If there is no explosion after 30 minutes, the safe is rated for one hour. If there is no explosion after 45 minutes, the two-hour rating may be assigned. The safe is then allowed to cool and the locks and parts fastenings are examined to determine whether the safe is still secure. The contents are examined for usability.

3. Fire Impact

After the explosion hazard test, the safe is removed from the furnace and within two minutes is dropped 9 metres onto brick riprap on a heavy concrete base. The unit is then examined to see whether the impact bent or ruptured parts that could allow exposure of the insulation or the interior walls. The unit is then allowed to cool. After cooling, the unit is heated again to 843°C for 30 minutes for a one-hour rating or 908°C for 45 minutes for a two-hour rating. After impact, the unit is again examined for deformation, rupture of parts, damaged insulation and any other openings into the interior. Once cooled, the unit's locking mechanisms and parts fastenings are re-examined for security and the interior examined for visible evidence of undue heat transmission.

Whether the safe has been tested for one or two hours is indicated by the labels U.L. Label/Class 350°F (176°C) one hour and Class 350°F two hour.

Other Features to Consider

- The safe should have a dual locking system (i.e., both a digital combination lock and a key lock). That way, in the event someone figures out the combination, a key is also required to obtain access to the stored data.
- Where should the safe be located in the office? The floor must be able to carry the weight of larger safes. This should not be a problem for most businesses with concrete floors. If you need to secure the safe to a wall or to the floor it would be prudent to ensure that anchoring is possible. Concrete floors may need to be drilled and tapped. Anchoring to a wall may be useless if the wall is using two-by-four studs with a dry-wall cover.
- A larger safe that would satisfy the needs of most business storage requirements has exterior dimensions of 144 cm high x 63 cm wide x 66 cm deep. A safe this size weighs about 500 kg.
- What are the size and number of documents to be stored in the safe? Although safes look large, the outside dimensions belie the interior capacity. For example, the external dimensions given in the previous bullet are for a safe with interior dimensions 89 cm high, 50 cm wide and 66 cm deep.
- Cost of the safe obviously depends on the size and rating of the safe. A safe with the above dimensions should run just under $2,000.
- Locking mechanisms may be important if one is considering storing diamonds or other high-value items; for most business applications, however, the locking bolts that slide out of the door into the side wall of the safe are more than adequate.
- The higher-end safes will be constructed with high-density shells that take up to 15 minutes to penetrate and will also be constructed with punch-resistant handles and locks and a tempered-glass relocking mechanism that blocks retraction of the main bolt, or blocks the door from opening if the primary locking mechanism is defeated.

The High Cost of Saving Money

Loss through theft or fire of proprietary data, unsecured credit cards, original documents establishing loan contracts or rights to insurance claims may never happen to your business. But….what if it does?

Cost of Purchase v. Cost of Loss

Before shopping for a safe, balance the cost of the loss of irreplaceable original documents with the cost of the safe. The loss of the day's cash receipts, corporate credit cards, negotiable instruments, backup drives, corporate financial statements, proprietary corporate information, confidential employee data, partnership or shareholder agreements, original documents of incorporation, mortgages, insurance policies, etc. can have a significant impact on the conduct of your business. A one-time investment in a safe to protect documents is an inexpensive means of securing your business.

BUSINESS MATTERS is prepared bimonthly by the Chartered Professional Accountants of Canada for the clients of its members.

Richard Fulcher, CPA, CA – Author; Patricia Adamson, M.A., M.I.St. – CPA Canada Editor.

Contact us: patricia@adamsonwriters.ca