

THE ONTARIO REPORT



SUMMER 2008
www.canasa.org

An official publication of CANASA's Ontario Chapter

Worker Safety is the Law

By Lance Naismith

It's hard to make a buck today with rising fuel costs savagely biting into most companies' profit margin.

One way to ease this burden is by taking all jobs that come available and push for volume. But in this rush to make up for lost profit, don't forget the one thing that can put a major crimp in anyone's business: Site safety. Regardless if you're working on a large complicated multi-million dollar project or a small one-man job, knowing your responsibilities regarding labour safety can mean the difference between success or a criminal prosecution.

"The employer has a duty to ensure his or her workers are trained and perform the work safely," notes Doug McVittie, the assistant general manager and director of operations for the Construction Safety Association of Ontario (CSAO). He notes that most employers are well intentioned and will listen to their workers if there is a problem. For workers, such as security system installers, there is a high level of trust by the employer and, although the employer must supply the training and tools, it is up to the worker to notify the employer of any work safety hazards.

According to McVittie, the biggest risk for security contractors falls, specifically from ladders. "We need to instill in everybody the idea of do it right each time, every time, all the time."



Under Ontario's Occupational and Health Safety Act, a "Constructor" is a person who undertakes a project for an owner and includes an owner who undertakes all or part of a project by himself or by more than one employer. No matter the size of the project, McVittie says that although contractually obligated, it is "good practice" to make contact with whoever is in charge of the facility, as they are responsible for safety compliance and notifying the Ministry of Labour of any projects/accidents.

For those performing work requiring "personal fall protection" training (e.g., bucket trucks and boom lifts working higher than 2.4 metres or construction sites), the CSAO offers a do-it-

yourself training package. The "Constructor" will require evidence of such training.

Ontario has very stringent regulations with large penalties (e.g., \$500,000 and 12 months in prison) for non-compliance. Other jurisdictions have less punitive consequences

To deal with worker safety — and in response to the 1992 Westray mine disaster and subsequent lack of penalty — Canada's Bill C-45 (CC 217.1) was developed, written and passed. Those who undertake or have authority to direct how another person does work is under a legal duty to take reasonable steps to prevent bodily harm. Failure to comply opens individuals and corporations up to unlimited penalties. Recently, a Quebec manufacturer, Transpave Inc., was the first Cana-

dian company to be convicted under Bill C-45.

To limit liability, a worker/supervisor or owner can contact the CSAO for advice or, if they consider the work too dangerous, the Ministry of Labour for a ruling. If you establish an effective occupational health and safety management system with regular audits, prevent bodily harm and ensure compliance with applicable occupational health and safety statutes and regulations, your risk management will reduce cost, injuries, worker downtime and increase job enjoyment.

If any workplace accident or injury occurs, you should contact local authorities to clarify jurisdiction or specific legislation.

IN THIS ISSUE

Lien on Me2

Ontario Executive

Report2

Understanding Your

Client's Needs3

Calendar of Events3

Database

Marketing4

Lien on Me

By Lance Naismith

For some, a firm handshake is still a way to conduct business, but under certain (and most) circumstances, it makes good business sense to follow legal procedures, such as Ontario's Construction Lien Act.

The Act, which allows those who perform construction work or supply materials for the construction, repair or alternation of buildings or land to protect their financial interests in the project, is designed for use, separately, from any other legal recourse (e.g., lawsuit). Whether a company utilizes the Construction Lien Act or not has no bearing on its ability to proceed in a court of law using other methods.

"The original intent was to provide the little guy the ability to get paid," notes Mel Gedruj, CSPM, a director with V2PM Inc., adding it allows security system suppliers, installers and integrators to protect their interests without having to resort to other, more costly methods.

According to the Act, companies can proceed under a process called "sheltering," whereby a number of claimants proceed under one claimant and share the costs. Utilizing the lien gives security contractors a secure claim against the land in case of

insolvency; it also will hinder construction financing, thus putting pressure on the contractor to pay. Furthermore, it tends to be less expensive than normal civil actions, although the Act does include penalties for false or inappropriate liens.

To ensure companies maintain their right to register a lien, there are certain timelines that must be followed. It is a good idea to have the correct information on hand from the start of a project, so that it can get started and proceed quickly. For some, the mere establishment of the lien will cause payment, as the owner does not want a lien on a property that will affect its value and sale potential.

Once a company has provided work, service or supplies to a project, the right to a lien is established. This right will expire, however, unless it is registered within 45 days after the last substantial supply of services or materials. Due to associated costs, most liens are filed close to the 45-day limit. The lien can be discharged by the disputed amount being paid into the court, awaiting a future ruling. When dealing with the timelines, it is advisable to contact a lawyer.

Basically, when a company submits a bill

for services, it will be paid, minus a statutory 10 per cent holdback only payable when substantial completion is obtained. If payment is not made, a lien is an option.

The lien of a contractor expires after 45 days based on the earlier of either:

- The date of publication of the certificate or declaration of substantial performance of the contract; or
- The date the contract is completed or abandoned.

This is usually the case for those working on a "lump sum contract." Gedruj points out that some individuals or firms may be directly retained by the owner and although they work for the general contractor for safety and payment purposes, the owner may pay the firm prior to substantial completion. The 10 per cent holdback and right to lien would still exist.

In today's highly competitive and litigious world, a handshake doesn't carry the same weight it used to, which is why a lien helps protect everyone's interests.

This article is meant for informational purposes only and is not to be taken as legal advice. Please contact a lawyer for further information.

ONTARIO EXECUTIVE REPORT

These are very exciting times within the security industry, particularly as new initiatives continue to be discussed and launched, and CANASA continues its positive growth. Our members are always developing new ideas and events, which are all focused on helping CANASA, and the security industry, as a whole, grow.

Currently, the Alarm Response Committee, chaired by Paul Georges, vice-president of CANASA's Ontario Chapter, has been working on the new false alarm policy in Durham Region. The committee has received tremendous support from Angelo Bucciarelli from UTC/Counterforce and Ken Mitchell, CANASA's executive director, whose contributions will no doubt help our entire membership. It is important for anyone conducting business in the Durham Region to get an updated copy of the bylaw, as it impacts the industry in many ways. For anyone who needs a copy of the policy, they are available at the CANASA office.

We would like to offer our congratulations to the SWO Sub-Chapter (London) for hosting another amazing golf tournament on June 20. The Ontario Chapter is working hard to ensure its upcoming event, scheduled for July 17 at Station Creek Golf Club in Gormley, Ont., is a resounding success as well. The Ottawa Sub-Chapter's golf tournament is scheduled for August 27. These events always present a great opportunity to get acquainted with your colleagues, as well as discuss industry issues, in a casual and informal setting.

We would also like to introduce the newly formed Monitoring Station Committee, which will be working on improving alarm central stations throughout the entire industry. Chaired by Bert O'Grady, the committee is accepting new members.

It should also be noted that Neil Jones has begun efforts to revamp and stream line our education programs. This will help bring more qualified candidates into the industry, and provide a higher level of industry standards for those already toiling in the security arena.

Jamie Couper, chairman of CANASA Ontario Tradeshow Committee, and his team are busy working with the staff at CANASA's national office to develop another informative conference, scheduled for October 22-23. The 2008 Security Canada Central event is expected to host the most progressive and educational security seminars in Canada. We hope that you mark these dates in your calendar, and plan to attend both days of the show.

I would be remiss if I did not say a special thank you to Rita Murphy, Chris Webb and Mel Gedruj for all their efforts on the CANASA newsletter. Having this newsletter definitely increases the communication to Ontario members and throughout the CANASA board. It is a vital source of information on all of our current initiatives.

I hope you enjoy this edition of *The Ontario Report* and remember, your comments are always welcome.

— Jamie Couper

UNDERSTANDING Your Client's Needs

By Mel Gedruj, CSPM

CANASA is the leading security industry association in Canada. As members, we are in business to serve our ultimate customers — the end users. In order for them to determine their security needs, there are specific tools and techniques available in the marketplace.

The two most widely used tools for security capital planning are security assessments and the security master plan.

Let's assume that we are dealing with one building or even two existing buildings (e.g., office, warehouse, plant, etc.). The first order of business would be to carry-out a security vulnerability assessment, also known as a Physical Security Assessment or Security Audit. It may be also be known by other names, but the concept is usually very similar.

For facilities not yet built — those still at the drawing board stage — a similar process may take place, but the focus would be on planning for security. Although the assessment is not a scientific process, there is typically a methodical approach that is needed — one that requires judgement on the part of the assessor and one that does not necessarily require an absolute accurate evaluation as long as it is properly documented and all assumptions recorded.

Two assessors may not see, rate or evaluate the same threat/vulnerability in an identical fashion. If the expertise is available in-house, end users can handle their own assessment; if not, retaining the services of independent professionals with no vested interest in products or systems is where members of the security industry come into play.

Briefly, here are the steps a security assessment might follow:

- Identify assets (e.g., people and real estate) and describe them;
- Identify current security measures, if any; this will encompass both systems and management procedures (e.g., incident reporting, key management, CCTV policy);
- Identify threats or adversaries likely to cause damage, harm and/or loss;
- Risk or threat vulnerabilities analysis is used in assessing the probability of a loss when faced with a given threat; vandalism could be specific to an area of a city and occur after

business hours, so if the frequency of that event is documented then the likelihood of this repeating itself is very high and should be recorded as such; and

- End user's risk tolerance; ultimately, the risk acceptance resides with the owner and/or end user of the facility being assessed. If after demonstrating that a risk has been identified and the consequences gauged, we have to ascertain whether it is to tolerable (e.g., potential loss acceptable or likelihood of event is remote) or unacceptable. The reason for such an analysis is to define and design the countermeasures to suit the client's needs. For instance, if a business owner does not want to use CCTV footage for prosecution, then high-resolution cameras are not really required, but if they want the ability to zoom into license plates and read them clearly, then video camera specifications must be reflective of that requirement.

Security assessments should result in a clearly articulated report outlining any assumptions, list of assets reviewed, people interviewed and sources of information. It should cover operating conditions, opening hours, key management and control, and open/close procedures, if applicable. The report should contain recommendations for counter measures. The latter would be comprised of proposed systems to be deployed for access control, CCTV, alarm configuration and network needs. (It is also important to list the proposed new or enhanced procedures for incident reporting management and key control, just to name a few.)

The security assessment is a fundamental tool for the development of a defensible capital plan. It enables the end user to submit a capital funding request internally; one that is based on clear priorities that can help the powers that be decide on the execution of that particular project.

Finally, organizations with a larger real estate portfolio would use a strategic tool known as the Security Master Plan. It involves establishing common criteria for the various assets in matters of threat and vulnerabilities and the corresponding countermeasures. For example, if we rate building "A" as high risk because of its use and location, it would qualify for package

CALENDAR OF EVENTS

July 17, 2008

Ontario Chapter Golf Tournament
Gormley, Ont.

August 27, 2008

Ottawa Sub-Chapter Golf Tournament

September 3-7, 2008

CEDIA Expo
Denver, Co.

September 11, 2008

Security Canada Atlantic
Moncton, N.B.

September 15-18, 2008

ASIS Seminar
Atlanta, Ga.

October 22-23, 2008

Security Canada Central
Toronto, Ont.

October 29-30, 2008

ISC East
New York, N.Y.

WE WANT TO HEAR FROM YOU!

The Ontario Report is your newsletter so if you have any article ideas, suggestions or opinions you want to share with us, please contact CANASA's national office at staff@canasa.org

**Next issue is scheduled for
release in Fall 2008**

"Type 1," which would include the maximum security package deployment possible within the portfolio.

The Master Plan is strategic, the Security Assessment is tactical and they both provide a roadmap for establishing the scope of security projects. The Master Plan allows end users to make decisions that would not harm future growth and expansion in their real estate portfolio, while individual assessments drill down to the finer details.

There is no doubt in my mind that end users and owners greatly benefit from approaching security as a management function requiring a defensible business planning process. It is for this reason that security assessment and planning is vital to the success of every business.

CANASA

610 Alden Road, Suite 100
 Markham, ON L3R 9Z1
 Phone: 905-513-0622
 Toll-Free: 1-800-538-9919
 Fax: 905-513-0624
staff@canasa.org
www.canasa.org

CANASA ONTARIO CHAPTER BOARD 2005 - 2008

Edward Fitchett, President
efitchett@fitch.ca

Paul Georges, Vice-President
pgeorges@purnrg.com

Jamie Couper, 2nd Vice-President
jamiec@ghcsafetyandsecurity.com

Sean Baghai, Secretary
seanbaghai@rogers.com

Mel Gedruj, Treasurer
melg@v2pm.com

Mark Fairley, Board Member
mark@tmfsecurity.com

Rita Murphy, Board Member
ritamurphy20@sympatico.ca

Bert O'Grady, Board Member
bert@lanvac.com

Al Herrington, Board Member
jherrington@can.rogers.com

Frank Filice, Board Member
frank@anaconsolutions.com

Neil Jones, Board Member
neil.jones@voxcom.com

Mary Vella, Board Member
mary.vella@apidealers.com

Travis Firth, Board Member
tfirth@tri-ed.com

Chris Webb, Board Member
cwebb@logenex.com

Paul Bentley, TAOL Representative
office@taol.net

COMMITTEE CHAIRS

Golf: Ed Fitchett

Response: Paul Georges

Education: Neil Jones

Self-Regulation: Mark Fairley

Nominating: Mark Fairley

Members' Meeting/
 Social: Frank Filice

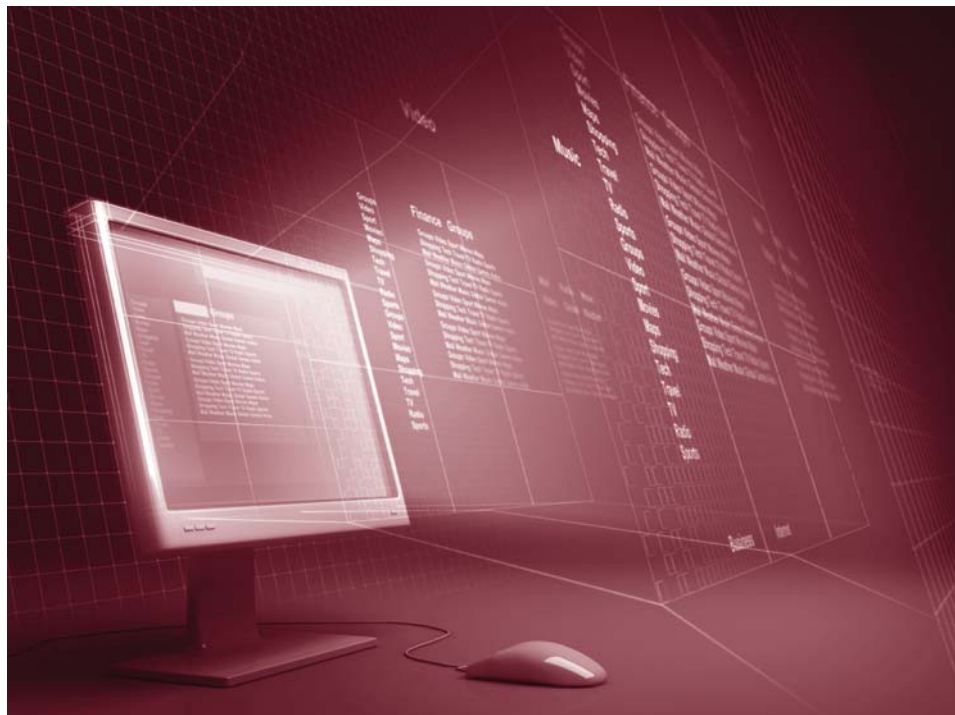
Media: Rita Murphy

Trade Show: Jamie Couper

Membership: Kolin Lee

Monitoring Station: Bert O'Grady

DATABASE MARKETING



Whether you're a partner in a consulting firm, a house painter or president of an international conglomerate, database marketing is vital to the success of any business. Database marketing can be simple or sophisticated. The key is that instead of just having a mailing list of prospective customers or a single list of current customers, you can use a computer to evaluate and manage the information more precisely.

For example, you may want to send a reminder mailing to every customer once a year; a monthly mailing to more active customers; and even place a phone call from time to time to your very best customers.

Here are some tips to start using your database as a powerful marketing tool:

TIER YOUR PROSPECT BASE

One of the primary rules of database marketing is spend most of your money hitting your best customers repeatedly, but save a little to experiment with new target groups. It is also important to make follow-up phone calls to your very best prospects and to previous customers who didn't order this year.

USE A MIX OF MARKETING VEHICLES

Historically, database marketing relied, overwhelmingly, on direct mail. Then came telemarketing and now there are a slew of alternatives to consider, including e-mail, fax,

and the Internet. For closing sales for higher-ticket goods or services, a combination of several different contact methods may work best. Be warned though, when conducting any type of marketing initiatives, be cautious of legal restrictions that prohibit companies from sending unsolicited faxes to people or companies with whom they don't have a business relationship.

FANCY AND EXPENSIVE DOESN'T ALWAYS SELL!

Make your mailing pieces professional and clean, but don't go overboard. Generally, a one-page letter, a two-to-four page flyer with two colours at the most, and a business reply card are all you need for an effective mailing. Avoid using mailing labels; address the envelopes yourself or have a mailing house do it by computer. As well, make sure you have a "call to action" in your letter, like a free evaluation, a free gift, or a limited-time deep discount.

TEST, TEST AND TEST SOME MORE!

In database marketing, changing even a small variable can wildly change your results. So once a mailing works for you in test quantities, do the exact same mailing to the exact same mailing list in larger quantities. When you do tests, isolate one variable at a time.

Source: Streetwise Business Tips