

## What's Inside

Page 1  
Social Engineering

Page 2  
Social Engineering Continued

Page 3  
New Clean Water Act

Page 4  
Renting a Vehicle in Ontario

Insert  
Suggested Guidelines for Creating a  
Culture of Security

## How many “outsiders” have access to your financial accounts? The answer could be surprising.

### Social Engineering - Can Your Employees Be Hacked?

*Our physical security initiatives serve to create an “illusion of security”.*

We are all familiar with the term “hacker” and we associate hacking with penetrating our computer security to obtain access to our electronic information. To protect ourselves we spend large sums of money on securing our network and our systems. We install firewalls, intrusion detection systems, authentication devices, anti-spam software, anti-virus software and the list goes on. As security vulnerabilities are announced we install the recommended patches within the recommended time frame. We continue to upgrade our security as new technologies become available spending even more money. Yet, we remain totally vulnerable!

A security system is only as strong as its weakest link. Often, the weakest links are people. Organizations are “customer service” driven. Their employees are trained to respond to customers’ inquiries as quickly as possible and without inconveniencing the customer. Yet, do we train our employees in what is considered appropriate versus inappropriate customer response? How do we protect our stakeholders’ information from being released to a third party by an inadvertent but accommodating employee action? Do our employees accept someone’s word over the telephone? Is a callback required when a change of banking, change of name or change of address is requested?

### *Have we trained our employees to be aware of the social engineer?*

“Social engineering” is the human side of stealing information or assets. It can be defined as outsiders tricking insiders to perform illicit acts such as allowing inappropriate access to corporate systems or providing proprietary information. Social engineers use influence and persuasion to engage an employee in committing a fraud. An employee unknowingly gives away information in an email, answers questions over the telephone to someone they don’t know, or follows directions to make changes to a stakeholder’s account without verification. It is not a new concept. It has been inferred that social engineering tactics placed the wooden horse behind the walls of Troy. The social engineer is a “con man” who exploits human vulnerabilities such as an individual’s desire to be helpful.

---

Social engineering attacks can be computer-based or human-based. Examples of computer-based attacks are email attachments containing malicious software, phishing or a counterfeit pop-up window. Human-based attacks exploit human nature. The information is obtained by asking questions of trusting employees, through impersonation, wandering through premises unescorted to observe employee workstations (looking for the yellow sticky note with the password stuck to the computer), obtaining employment within the organization, dumpster diving and studying the information on corporate websites.

### ***How can the organization protect itself?***

Successful social engineering attacks rely on the employees of the organization. Organizations need to create a culture of security through clear and strong security policies and “standard operating procedures” to guard against social engineering. Employees must be trained in recognizing social engineering attacks and trained in the organization’s policies and procedures. Security companies advise that up to 40% of an organization’s security budget should be spent on employee training.

The first step in preventing an attack is “spotting” the attack. Some signs of an attack by a caller are:

- *Caller refuses to give contact information*
- *Caller rushes through the request*
- *Name dropping throughout the conversation*
- *Resorts to intimidation when questioned*
- *Asks “odd” questions*
- *States a senior member in the organization needs the information now*
- *Requests confidential information*
- *Requests changes to confidential information*

This list is by no means exhaustive and we recommend that organizations work with security firms that specialize in training employees against social engineering attacks.

Though the telephone is a popular method of gaining “inside” access, it is not the only method used. How many “intruders” are allowed to wander through your organization in a given day? Does anyone question the telephone repairman, computer technician or electrician? How about the well-dressed individual who appears to belong?

### ***Not All Risks Faced By The Organization Are Insurable***

The organization can suffer a financial loss as a result of a social engineering attack and find itself without an insurance recovery. Money and securities are not covered property under a Property Policy. Employee Dishonesty coverage responds when an employee steals from the organization but not when an employee is used unknowingly as a pawn in the commission of fraud. Errors and Omissions Policies respond to third party financial losses not to first party losses. Since there is no bodily injury or property damage the CGL is not involved.

Only by creating a culture of security and implementing reasonable controls can the organization take a proactive defense against social engineering attacks. Why is this necessary? Because times have changed.

---

## ***CLEAN WATER ACT: WILL NEW ROLES AND RESPONSIBILITIES MEAN GREATER LIABILITY EXPOSURE?***

*Christine Carter is a partner at Paterson, MacDougall and is the author of the chapter on Environmental Liability in "The Law of Municipal Liability in Canada". She can be reached at (416) 643-3304 or ccarter@pmlaw.com*

As the new Clean Water Act winds its way through the legislative process, many municipalities and conservation authorities are grappling with the potential implications. While the legislation is not yet in its final form, it has become apparent that both the financial implications and the potential for increased liability exposure could be significant.

On December 5, 2005, the Ontario Government tabled the Clean Water Act, 2005 in response to recommendations of the Walkerton Inquiry. The stated purpose of the Act is to protect existing and future sources of drinking water.

The Act establishes drinking water source protection areas throughout the province and requires that "source protection committees" prepare assessment reports. Since the source protection areas are watershed based, the committees will be composed of municipalities, conservation authorities and other stake holders within that area, thereby somewhat blurring the traditionally, well demarcated existing municipal, regional and conservation authority boundaries.

Once the assessment plan is complete, the source protection committee is required to develop a source protection plan, setting out how it intends to eliminate significant drinking water threats. This process will include identifying existing or future land use activities within a well head protection area which pose potential drinking water threats, then regulating land use in ways never before contemplated. The obvious financial and staffing challenge for municipalities will be identifying employees with sufficient clean water/watershed expertise combined with land use planning knowledge. From a land use planning perspective, municipalities may find themselves involved in disputes ranging from appropriate land use of the local dry cleaner to regulating discharge of contaminants from large multinational industries within their municipal or watershed boundaries. In all likelihood new "clean water" departments and specially trained employees with these additional responsibilities will have to be established by municipalities. Municipalities and conservation authorities may take some comfort from the fact that the provincial government has set aside funds over the next five years to provide grants.

Of most significant concern is the requirement that each source protection committee prepare an assessment report identifying not only all watersheds in the area but also all "vulnerable areas within the watershed" as well as "drinking water threats in each vulnerable area". While this is of course a laudable goal, and a necessary step to eliminate potential drinking water health threats, the entire process is public, including publication of the assessment plan. The difficulty with this approach from a liability perspective is that once the risks have been identified in a very public fashion, the potential for actions and the likelihood of large class actions arising also increases. While some immunity is provided to municipal employees with respect to acts done in good faith in enforcing the provisions of the Act, it is not clear to what extent municipalities or conservation authorities will be shielded from the consequences of drinking water threats they were not previously aware even existed within their boundaries.

The Bill has now received second reading and is scheduled to receive royal assent in the fall. Municipalities and conservation authorities are well advised to begin assessing their needs and exposures and consider developing risk management strategies to address these issues as the date approaches.

---

## *Renting a Vehicle in Ontario - The Rules Have Changed*

The Ontario Government passed Bill C18 on March 1, 2006. Bill C18 makes persons renting or leasing vehicles in Ontario, “first in line” to pay in the event of an accident resulting from the negligent use or operation of the leased/rented vehicle. Prior to Bill C18, the Leasing or Rental Company (the owner of the vehicle) was the first to respond to a similar incident.

The new responding order to accidents with rented/leased vehicles is:

- The insurer of the lessee or renter under a contract of Automobile Insurance, where the lessee or renter is a Named Insured under the contract
- A driver’s policy or ‘drive’ other automobile coverage
- The insurance of the owner of the vehicle (the rental or leasing company), which would only pay in excess to the above mentioned policies. The Act also caps the amount that the Leasing Companies are responsible for to generally \$1,000,000, subject to conditions.

While municipalities frequently rely on rental or leased vehicles for their daily business, the vehicles are often rented in the name of the individual employee and not the municipality proper. Under Bill C18, if the employee rents the vehicle in his/her own name, the employee’s personal auto policy will be called upon first to respond to an accident with the rented vehicle.

The following examples illustrate the responding auto policies in two different scenarios.

### *Scenario 1*

The employee of Municipality A rents a vehicle in the name of Municipality A and is involved in an accident while on municipal business.

- The Insurer of Municipality A pays first
- If the claim exceeds the Municipality’s limits, than any policy where the employee driver is a Named Insured, spouse of the Named Insured or a Named Driver pays next. This would be quite rare in view of the limits most Municipalities purchase.
- If any claim remains, the Rental Company would be next to respond. However, due to the \$1,000,000 cap and the corresponding conditions, it is unlikely to respond.
- Non-owned Auto is in excess of the policies listed above. This is not by virtue of Bill C18 but rather driven by the wordings.

The ability for the employee to rent a vehicle in the name of the Municipality will have to be pre-arranged with the rental/leasing company. The employee will not typically have signing authority at the counter.

### *Scenario 2*

The employee of Municipality B rents a vehicle in his/her own name and is involved in an accident while on municipal business.

- The employee’s personal auto insurer would respond first. If the employee is listed on Municipality B’s fleet policy, this policy would pro-rate with the employee’s policy. If the employee has a spouse with a policy or is a named driver on a policy, that policy would also pro-rate.
- If any claim amount remains, the Rental Company would next respond. However, again due to the \$1,000,000 cap and conditions, this is most unlikely to occur.
- Non-owned Auto is in excess to the policies listed above. As mentioned in Scenario 1, this is not because of Bill C18 but rather driven by the wordings.

#### **Frank Cowan Company**

4 Cowan Street, East  
Princeton, ON N0J 1V0  
Toll free: 1-800-265-4000  
Phone: (519) 458-4331  
Fax: (519) 458-4366

[www.frankcowan.com](http://www.frankcowan.com)

---

# Suggested Guidelines for Creating a Culture of Security

- Appoint a person within the organization who will be responsible for coordinating the creation and the implementation of the policy and procedures.
- Include your employees in the creation of these policies. They are a valuable resource and can make valid contributions. If they are involved in policy creation they will understand the reasons behind and the importance of such policies and they will take ownership.
- Establish an employee participation program by encouraging employees to report security breaches
- Protect “whistleblowers”
- Develop simple rules to define what information is sensitive/confidential
- Write the policies in simple language and avoid IT “jargon”
- Post the policy on your intranet
- Encourage department managers to explain the policy to their employees
- All employees should sign an acknowledgment form that they have read the policies

## Physical Security of the Premises

- All visitors, contractors, suppliers should be required to report to the receptionist
- The receptionist should have a list of the contractors and suppliers that will be on premises on a given date
- If a technician arrives who is not on the list, the appropriate department should be called to verify his/her presence
- There should be a sign-in sheet that includes Name of Company, Name of Person, Employee Contact, Time In and Time Out
- All outside personnel should be given ID Badges
- After receiving an ID Badge they should be escorted by an employee
- Shredding information - strict guidelines on what information must be shredded and not “thrown into the garbage”
- Dumpsters - rather than being accessible to the public they should be stored in a secure area to avoid “dumpster diving” for sensitive information

---

## Securing Customer/Supplier Information

- The policy should detail who can release information to the public and under what circumstances
- Requests for address changes should only be accepted if they are issued by the customer or principal of the supplier's firm
- The request should be in writing
- A callback for all corporate address changes should be required
- Banking information changes for electronic transfers should not be allowed over the telephone
- All changes for electronic transfers should be required to be made in person by an individual that is authorized to make such changes on behalf of the corporation and providing appropriate identification
- The name of such person should be on file along with the other signing officers
- Before initiating the change, a callback should be made to another signing officer of the firm
- Banking information changes involving electronic transfers should be the responsibility of senior staff members of the organization
- Suspicious phone calls should be reported

## Employee Password Policies

- Change all default passwords
- Don't allow passwords based on personal information
- Don't allow passwords based on words found in the dictionary
- Passwords should incorporate lowercase and CAPITAL LETTERS
- Passwords should incorporate letters and numbers
- Employees must safeguard their passwords
- Passwords should never be given to anyone over the telephone
- Passwords shouldn't be written on a yellow sticky and stuck to the computer
- Employees should not share their password with anyone else in the office
- Make employees change their passwords every 30 days
- Don't allow the same passwords to be used within a 24 month period
- Instruct all employees to use caution with email attachments
- Remove unused user accounts
- Users should lock their computers when away from their desk
- Out of Office Message - restrict who it is sent to
- Employees should not be allowed to discuss the organization in personal blogs

## Policies Should Also Address:

- Internet Cafes
- Chat Rooms - discussing the organization
- MSN during Business Hours
- Personal use of corporate systems
- Modems
- Personal Portable data storage devices such as iPods, Memory sticks etc
- Camera Telephones