By Ingrid Sapona | 19-minute read

In this issue we focus on two topics that have made news in the last six months. The first one – revisiting the need for overland water coverage – arose (no pun intended) as a result of flash floods that were a side-effect of the June 13 hail storm that hit Calgary and surrounding communities. The second topic is the increased incidence of social engineering fraud that has surfaced during the pandemic.

Revisiting the need for overland water coverage

"[The] lack of knowledge about how flooding occurs can translate to clients not appreciating the risks, which is why broker and customer education are so important."*—Amy Graham, RSA Canada*

Hailstorms in Calgary are fairly common. According to Barry Haggis, president of Young-Haggis Insurance Service Ltd., in June of this year alone, Calgary had 21 hail days. “We know when it’s coming. We do our best to prepare for them with alerts about where they’re likely to be. We even have the Alberta Hail Suppression Project, which sends up planes to seed clouds in an effort to reduce the size of the hail. But this one just came so fast,” he said about the June 13, 2020 storm.

Indeed, the storm that hit the northeast section of Calgary, Airdrie, and Rocky View County that day was declared an “extraordinary event” by Alberta Premier Jason Kenney a few days later. It proved to be one for the record books. With over 70,000

claims filed related to the storm, estimates are that the P&C industry will pay out nearly $1.2 billion for repairs related to the storm. That makes the event the fourth-costliest insured disaster in Canadian history.

Initial photos and videos of the storm damage showed cars with all the windows smashed, homes with shredded roofs and siding, broken windows, and yards covered in what looked like large snowballs. While that was what most people saw when they looked out their windows, the storm also brought flooding because sewers got overwhelmed. Indeed, the heavy rain that accompanied the hail and flooded the streets causing what is commonly referred to as overland flooding.

Overland water coverage typically covers damage caused from freshwater sources that enters a building at ground level, for example, through a basement window or a crack in the basement wall above grade, or through the garage.

Sewer backup coverage typically covers water damage within the dwelling caused by back up from a sewer in situations where there's no external flooding touching the insured's premises.

According to the Premier, "Nearly 400 homes and small businesses suffered some over-the-surface flood damage, at least 20 were filled to the main floor with water…". Because the Alberta Emergency Management Agency classified the storm as an extraordinary event, individuals and businesses that suffered damages caused by overland flooding were eligible for disaster relief funding so long as their losses were uninsurable. Kenny also made it clear that Albertans who could have purchased insurance coverage for overland water but who didn't, or who had an inadequate amount of coverage, were not eligible for funding.

This helpful flood event checklist published by the Canadian Red Cross includes a list of provincial and territorial authorities for coordinating relief with various disaster recovery programs across Canada.

The flooding from the storm provided vivid proof of what many Canadians don't seem to appreciate: that just because a property isn't on the banks of a flowing river, doesn't mean it can't suffer damage due to flooding caused by overland or surface water. A study conducted by RSA Canada and the World Wildlife Fund Canada (WWF) in August 2019 showed that 74% of Canadians agree that flooding has increased in Canada, and also revealed that 29% believe flooding only occurs in low-lying areas and 19% believe it occurs only near a body of water. Nonetheless, 31% of Canadians are worried they'll be affected by floods in the next 12 months.

Amy Graham, National Property Underwriting Manager, Personal Insurance for RSA Canada, said there was a push to educate people about flood coverage in 2015 when it was introduced. "Before coverage was available for 'freshwater flooding' – or 'overland

flooding' as it's sometimes called – most people thought sewer backup coverage was enough," she says.

When it was first launched some brokers, recognizing how important flood coverage is, asked insurers to allow them to add the coverage to all policies. "When the coverage was introduced, we were flexible with brokers, and customers as well, who asked us to add it to their policies because it was such important coverage," says Graham. RSA's current practice is that to get coverage, people have to ask for it – and they do. "I'd say we see about 80% of our new business purchasing Waterproof Coverage™. That's really strong," she says.

How coverage has evolved

"Since we launched flood coverage, we have continued to review and tweak it to address current realities," says Graham. "For example, the most recent change we made is to provide Loss Prevention Device coverage to help prevent future sewer backup losses with Waterproof Coverage™ in addition to the combined sewer backup and overland flood coverage. We did this because we wanted to make it as easy as possible to purchase, as well as helping to emphasize the importance of mitigation," she says. "At the same time, recognizing that there will be some policyholders who do not qualify for overland flood coverage or do not want the full coverage they have an option to purchase sewer backup coverage on its own as well," she says.

Other insurers also pair overland water coverage with other coverages. Wawanesa pairs overland flooding with sewer backup under one coverage, which it calls Water Defence Coverage. With Aviva, for example, overland water is optional coverage but it must be purchased with sewer backup.

(Re)-educating policyholders

Given how widely reported the June 13 Calgary hail storm was, and given the concerns Canadians clearly have about flooding, perhaps brokers should consider this opportunity to re-engage policyholders about flood risks and their coverage(s) related to water-related risks.

Haggis says that it's usually not a big challenge to convince policyholders to take out overland water coverage once they understand what it covers. And, it's clear that some policyholders find the different water coverages available confusing. "I've had people ask me if overland water coverage is for when your toilet overflows. They figure that it is, since such water flows 'over land'," he says. Haggis thinks that often the reason people decline coverage is because they don't understand what it is or they think that because of where or how their property is situated, "it'll never happen to them," he says.

A flooded basement costs an average of **$43,000** to repair, according to 2018 data from the Insurance Bureau of Canada (IBC).

Graham also points out that while the RSA-WWF study made it clear that Canadians are increasingly worried about floods, it also highlights some gaps in peoples'

knowledge. Interestingly, 77% believe flooding has increased due to climate change. But, when it came to other causes of flooding, 47% mentioned reduced absorption of water due to a lack of green space, and 27% did not know that paved surfaces lead to more water runoff. “This lack of knowledge about how flooding occurs can translate to clients not appreciating the risks, which is why broker and customer education are so important,” says Graham, “and which is why we created our Climate Smart website. ”
As everyone in the industry knows, the reasons policyholders decline coverage is as individual as the policyholders themselves. Haggis thinks that part of broker due diligence, however, is to ensure policyholders’ decisions are grounded in a solid understanding of the coverage options available. The fact that there were people in the Calgary area who could have bought coverage but didn’t could well be because they didn’t understand what it covered. “[I]t scares me to think how many people declined overland flood, thinking, ‘Oh, I am up on a hill’ or ‘This is never going to happen,’ or ‘I am far away from the river,’ or whatever the case may be,” said Haggis in an interview shortly after the storm.

Additional industry resources:

• Partners for Action FloodSmart Canada - information and resources on floods, flood risks, and emergency preparedness for Canadians.
• Institute for Catastrophic Loss Reduction (ICLR) Flood Resources - flood resources for homeowners, businesses, insurers, and municipalities.
• Intact Centre on Climate Adaptation Home Flood Protection Program - a residential flood risk reduction education program.

Of course, there’s always the possibility that premium is a concern. Graham says that RSA’s experience, however, is that premium is not usually the issue. “There are many ways cost issues can be managed. This is where broker advice is so valuable. You can select a lower limit of coverage, or increase the deductible, or install water mitigation, for example,” she says.

As with any additional coverage available to policyholders, renewal is a good opportunity to educate clients about the various coverages they should consider to ensure they’re covered for different water-related perils. Indeed, Haggis thinks from a broker liability point of view it’s important that at renewal brokers point out to clients who are eligible for such coverage – but who don’t currently have it – that they should consider it. “The first time a policyholder declines overland water coverage we actually ask them to sign a release and we keep that as part of their file,” he says.

“Then, every year, when we prepare the renewal letter, we look at the policy and see what coverages the client has and what they qualify for but don’t have. Then we customize the letter, specifying what additional coverages they don’t currently have but that we think they should consider. We also provide them with various cost and deductible options for such coverages and we indicate we’d be happy to discuss it and answer questions,” Haggis explains. “And of course, we keep a copy of that letter in the

file, along with any notes about discussions we may have had about the coverages. That way, if they come back later and say that they didn't know the coverage was available, we can show that we told them it was and that we suggested it to them," he says.

A few weeks after the storm, Haggis was quoted in *Canadian Underwriter* talking about potential reputational risk to the industry with respect to people complaining about how insurance companies responded. In the article, Haggis pointed out that there could well be instances of people complaining about a lack of coverage when, in fact, the client had declined the coverage. Haggis admits that after that article came out, he had second thoughts about whether he should have done that interview. "I worried that it might look like I'm simply siding with the insurers, but I've actually gotten a lot of positive comments from speaking up. Others in the industry have thanked me for standing up for the industry," he said.
While Haggis agrees that renewal is an important time for brokers to engage clients about overland water coverage, it's certainly not the only time his firm does. "Every spring, just before hail storm season begins, we send an email blast to clients reminding them to make sure they have overland water coverage. It's a generic note but about 55-60% of our clients respond. Most of them just phone and ask, 'I have this, right?'," he said. "And if they do call to ask, that's a terrific opportunity to talk with them about how important it is and to talk about the limits, the deductible, and all that," he says.

Record-breaking storms like the one that hit Calgary in June drive home to many the very real damage overland flooding can cause. Brokers should consider using that storm as a conversation starter with clients to drive home the risks of overland flooding and to make sure policyholders understand all the different types of water-related coverages available.

Social engineering on the rise: how to protect your business

Social engineering is the term used to describe a number of techniques used to perpetrate fraud by tricking people into voluntarily doing something, such as transferring funds, revealing sensitive information, or providing access to a computer network. Social engineering frauds are often carried out against businesses. According to Marsh

& McLennan, businesses of all sizes, industries and geographies have been victims of social engineering frauds. As Aon describes it, "social engineering refers to the use of identity deception to gain the confidence of an employee to induce him or her to part with an organization's money or securities."

Social engineering is a technique by which cyber criminals use psychological manipulation to achieve their goals.

Social engineering frauds are accomplished through human interactions. One hallmark of such fraud is that the "fraudsters aim to piece together information from various sources such as social media and intercepted correspondence in order to appear convincing and trustworthy while perpetrating the fraud." For example, the fraudster may impersonate someone the target knows, or pose as an authority figure (a government agent, for example) or a third party (perhaps a vendor the employer deals with). Given the rise of social media, it's easy for scammers to learn quite a lot about individuals – where they work, where they went to school, what social activities they're involved with, and so on. A fraudster then sends the target an email the target thinks is from someone in their social sphere and if they click on it – the fraudster is off to the races.

Though social engineering fraud can result in a fraudster gaining access to a business' computers and data, **it is different from hacking and other malicious** cyber acts that involve unauthorized entries into computer systems. With social engineering fraud, the fraudster **uses human interaction** to gain the trust of an employee who then helps the fraudster without realizing they have been duped.

Pandemic's impact on social engineering

There has been a marked rise in social engineering during the pandemic. The increase is largely attributable to the shift to working from home. Some businesses might not have as strict controls in place with respect to people working from home as they had in the office. Besides all the cyber security concerns with corporate data moving over the internet, and relatively insecure home WiFi, there is increased risk if family members access work computers. As well, over time, some workers become more relaxed in their home environment and they let their guard down. Others feel added stress from working at home or are anxious about COVID-19, which can translate to reduced vigilance. Scammers know this and so they've ramped up their efforts. Google reported more than 18 million daily email scams related to COVID-19 in a single week in April 2020.

Most common types of social engineering attacks

Risk Mitigation Methods

There are a variety of ways to mitigate the risk of loss from social engineering frauds, including employee training, requiring two-part authentication before making any payments, and insurance protection.

A growing field of cyber security research is focused on social engineering - that is, how to protect people from being manipulated into inadvertently assisting cyber criminals. Because of the escalating use of social engineering by attackers, companies are encouraged to establish a culture of security. Employee training is essential because such frauds are founded on human error. So, it's important that employees know more than just how to correctly log into a business' systems. They need to understand the ways fraudsters might take advantage of employees and they need to understand how their stress makes them even more vulnerable to such frauds.

Requiring two-part authentication is fairly common in login processes in the digital world, but it need not involve a high-tech solution. For example, a company could require that before anyone authorizes an electronic transfer of funds the person must separately contact someone else to verify that the funds should be sent. Or for employee-to-employee communications made over a public telephone network, a second factor, such as a unique phrase, might be required to authenticate the phone call before sensitive information can be discussed.

Insurance covering social engineering fraud has been available in Canada for since 2014. But, it's important for businesses to ensure they have coverage that specifically covers social engineering fraud, rather than assume such frauds would be covered under a computer fraud policy, a funds transfer fraud policy, or a commercial crime policy.

Standard computer fraud coverage is meant to cover unauthorized entry into, or use of, a computer system, in other words, hacks into a computer system. When an employee transfers funds as a result of falling victim to a social engineering fraud, a computer fraud policy doesn't respond because, even though the funds were transferred via computer, the transfer was caused by the acts of an employee, not as the result of a computer hack. Put another way, the use of the computer was merely incidental.

Fund transfer fraud coverage provides protection in the event of a fraudulent transfer caused by a third party directing a financial institution to transfer the insured's funds without the insured's knowledge or consent. With social engineering frauds, however, the transfers are made at the direction of the insured's employee, so the transfer is considered with the knowledge of the insured.

Commercial crime policies are meant to cover situations where an employee steals or benefits from a theft. But, in a social engineering fraud, it's not the employee who benefits. Crime policies also often specify categories of crime, so unless social

engineering is specified, it won't be covered. And some crime policies contain specific exclusions for losses resulting from authorised entry (by an employee) into the insured's computer system.

However, the insurance industry has realized the significance of social engineering fraud and coverage is specifically available for it. In some cases, social engineering coverage is available in the crime insurance marketplace, for example as an endorsement on a crime policy. Often there are sub-limits for such coverage, but if the insured can demonstrate that it has adequate controls in place, they might qualify for higher limits.

As with any insurance, when looking at social engineering coverage, companies should pay attention to any limits or loss qualifiers. Policy conditions should also be examined carefully, as there may be conditions precedent the insured must meet, such as having certain security policies and protocols in place to prevent the likelihood of such losses, such as robust employee training. As well, the coverage trigger provisions should be considered. Does it matter who the perpetrator of the fraud is? For example, does it only cover frauds committed by an individual, or does it cover frauds perpetrated by state actors? Does the policy cover the cost of information gathering to prove the loss, such as the cost of tech or forensic specialists needed to prove a claim?

Twitter's cyber incident this year was as a result of a "coordinated social engineering attack." The company confirmed in an update that cyber criminals targeted and successfully manipulated a small group of employees through a phone spear phishing attack, and used their credentials to gain unauthorized access to internal systems.

Social engineering frauds aren't going away – even if workers return to their offices. Businesses should ensure their employees are trained to understand the techniques social engineering fraudsters employ and their vital role in warding off social engineering attempts. As well, businesses should review with their brokers and risk managers their policy coverage and understand what is, and is not, covered.

Given that demand for insurance protection tends to lag surges in claims and given that social engineering fraud has risen sharply during the pandemic , the market for social engineering coverage should increase. Now is the time for brokers to familiarize themselves with the coverage and to consider how they might help protect their clients before they become victims of such fraud.