EPICCGRAM
EMERGENCY PREPAREDNESS FOR INDUSTRY AND COMMERCE COUNCIL
Volume 67 –September‘ 11

Stay Tuned in next month’s EPICCgram for a recap on the 7th Annual Victoria Seminar. It was a true Success!

With respect to earthquakes, we often get asked the question: how big of an earthquake can my building take? We often struggle with giving an answer that people would understand.

HOW BIG OF AN EARTHQUAKE IS MY BUILDING GOOD FOR?

Article by: **Dennis Gam, EPICC Director Read Jones Christofferson Ltd.**

This is a question we get asked a lot in these times of increased sensitivity to earthquakes due to recent world events. But the answer is not easily explained as the building code does not directly correlate building design parameters with Richter magnitude numbers. The National Building Code of Canada has typically based environmental loading on “event return period.” Environmental loads include wind, snow, and earthquake. Return period describes how often a natural event of certain intensity would occur. For example, the wind storm that devastated Stanley Park was described in the media as the “once in one hundred year” event. By comparison, buildings are typically designed for the “once in thirty year” wind storm.

For earthquakes, the 1990 and 1995 building codes were established around an event with a 475 year return period.

Some sources have informally suggested that this roughly represents a magnitude 7 event based on the seismicity specific to our region. The problem is that Richter magnitude is not a building design parameter, it is an expression of the amount of energy released by the earthquake. If that energy were released near the surface it would be far more damaging that if it was released deep underground. This fact is not reflected by the Richter magnitude number. In addition, the Richter scale not linear. Fifty percent of a magnitude 7 event IS NOT a magnitude 3.5 event. As such, it is almost impossible to extrapolate a Richter magnitude equivalency to some percentage of building code loading.

In 2005, for a number of reasons, the return period of the design earthquake was increased from 475 years to 2500 years. This roughly increased the design event to a magnitude 9 earthquake, which is expected to occur in the Cascadia subduction zone, west of Vancouver island, approximately 300km west of Vancouver. As such, although the Richter magnitude of the expected earthquake in the 2005 Code is bigger, the affect on the design parameters within Greater Vancouver does not increase by the same proportion or percentage.

Typically building design parameters are based on how buildings react to an earthquake ground motion. In general tall buildings perform better and react more favorably than short squat building types. It is impossible to indicate how a building would perform against the most current building code requirements without completing a quantitative analysis of the structure. However, most buildings built to “modern codes,” with a defined lateral force resisting system, have

typically performed well in earthquakes around the world. Buildings with a highly regular and symmetric plan footprint also have demonstrated better performance as well.

For more information on Earthquake Preparedness visit the website **www.epicc.org** or purchase the Earthquake Preparedness guide by calling **604.813.7979**

Seismologists in the aftermath of earthquakes

Maurice Lamontagne addressing the employees of the Canadian embassy in Port-au-Prince. Source: Natural Resources Canada.

In the aftermath of an earthquake, misconceptions and rumours are heard, repeated or read everywhere and very few people have the knowledge to filter the good from the bad information. Having a seismologist to provide the best information available and to answer questions can help the recovery process of some people.

As a seismologist, I specialize in the study of eastern Canadian earthquakes. Many of the earthquakes I studied, for example, the 1988 magnitude 5.9 Saguenay and the 2010 magnitude5.0 Val-des-Bois (north of Ottawa), occurred in areas considered “stable” by an unaware population. Because earthquakes happened so infrequently, most people were unprepared when an earthquake struck and did not react properly in those stressful few seconds. This low level of awareness can lead to an anxiety that may extend the recovery period. Over the years, I have discovered that specialists like me can help beyond the scientific work that is expected of them.

Seismologists can adapt their communication after an earthquake to make it more useful to a population in shock. Part of the post-earthquake fear arises from a lack of basic knowledge about earthquake processes and preparedness measures. Seismologists can use media coverage to deliver information that encourages people to act rather than passively face this hazard.

At the request of the Canadian Embassy in Haiti, I participated in the recovery of their personnel in Port-au-Prince following the tragic earthquake of 12 January 2010. I was part of a team mandated to install a seismograph network to record the numerous aftershocks that followed. My specific role, however, focused on helping people recover from that traumatic earthquake by dissipating misconceptions and rumours that circulated in the population. Using a PowerPoint presentation, I explained some basic concepts of seismology with emphasis on the January 12th, 2010 earthquake and the meaning of the aftershocks that people felt. People were hungry for factual answers to these questions: “Is this the precursor to an even larger earthquake?” “Can earthquakes be predicted?” “Can a tsunami follow a large earthquake?” “What can we do to better prepare for future events?” Helping people understanding the physical process is a first step towards calming their fear and rebuilding their confidence after such a traumatic event. Explanations on what to expect in the months to come, how to get prepared and how to react if another sizable earthquake occurred, empowered them to take care of themselves and their dependents. I felt humbled by the resilience and inner strength of the Haitian people. I made the presentation at five other occasions during my stay in Haiti. I was contacted by radio stations in Port-au-Prince to provide answers to the questions people had. Some responses to emails to residents even ended up on the web. Two weeks after the March 2010 Chile earthquake, I did a similar presentation via teleconference to the personnel of the Canadian Embassy in Santiago. Again people were happy to have direct contact with an earthquake specialist and were grateful that the embassy devoted time and efforts to ease their concerns. This shows that even in developed countries where access to the electronic media is common, many questions remain unanswered unless we, the specialists, become available.

I learned four key lessons from these experiences. First, in the Internet era, we should not assume people are getting the information they need or the correct answers to their questions. Misconceptions and rumours are heard, repeated and read everywhere and very few people can filter the good from the bad. Having an expert to answer their questions is an essential component to the recovery process. Second, people need to understand the basics about how earthquakes happen before they can go on to the next steps of their recovery. Having some rationale for something so sudden and unpredictable as an earthquake helps. Third, people need to be empowered and that comes from knowledge of how to protect themselves and their loved ones. By being active rather than passive, they can get back to normal faster.

Finally, seismologists have a role to play in communicating their knowledge to the public. Seismologists should adapt their communication to help the recovery of a population in shock. In an era of electronic communications where good and bad information exist side by side, direct contact with a specialist remains very valuable.

Maurice Lamontagne
Geological Survey of Canada
615 Booth Street, Ottawa, ON

Very Interesting and Untold Story of 9/11

Evacuation by Boat shows resilience of cities. Article by Christopher Mims, posted on smartplanet.com blog.

Here, in its entirety, is the incredibly moving, just-released, Tom Hanks-narrated, 11-minute documentary of the largest-ever evacuation by boat in history.

In nine hours, boats streaming in from all over the Northeast evacuated 500,000 people trapped on Manhattan Island by the complete shutdown of all trains and bridges in the wake of the fall of the twin towers. (Compare that with history's second-biggest evacuation, of 339,000 soldiers and civilians from Dunkirk, in WWII, which took nine days.)

One of the things this event illustrates is that in cities present and future, redundancy is one of the keys to resilience. New York has long neglected its waterfront, and in the face of rising seas it is even occasionally seen as a liability. And yet without access to the water, a half million New Yorkers would not have made it home on 9/11.

This documentary was produced by Road2Resilience, part of an effort by the Center for National Policy to "build the reflexes and instincts necessary at every level of American society to respond quickly and wisely to future crises."

Check the link to watch the video

http://www.smartplanet.com/blog/cities/moving-documentary-of-911-evacuation-by-boat-shows-resilience-of-cities/881?tag=nl.e660

Identifying Security Problems

An Article from the Wall Street Journal
By Geoffrey A. Fowler and Ben Worthen

Recent hacking attacks on Sony Corp. and Lockheed Martin Corp. grabbed headlines. What happened at City Newsstand Inc. last year did not.

Unbeknownst to owner Joe Angelastri, cyber thieves planted a software program on the cash registers at his two Chicago-area magazine shops that sent customer credit-card numbers to Russia. MasterCard Inc. demanded an investigation, at Mr. Angelastri's expense, and the whole ordeal left him out about $22,000.

Joe Angelastri, owner of City Newsstand in the Chicago area, is out $22,000 because cyber hackers attacked his stores' payment system.

His experience highlights a growing threat to small businesses. Hackers are expanding

their sights beyond multinationals to include any business that stores data in electronic form. Small companies, which are making the leap to computerized systems and digital records, have now become hackers' main target.

"Who would want to break into us?" asked Mr. Angelastri, who says the breach cut his annual profit in half. "We're not running a bank."

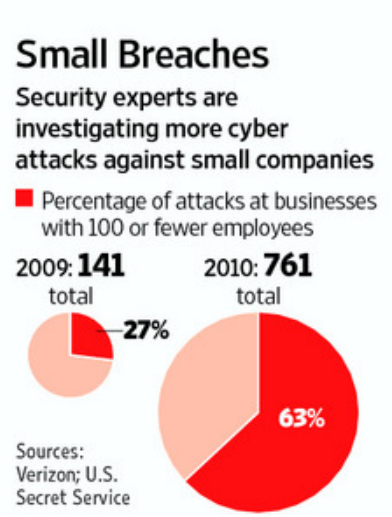
With limited budgets and few or no technical experts on staff, small businesses generally have weak security. Cyber criminals have taken notice. In 2010, the U.S. Secret Service and Verizon Communications Inc.'s forensic analysis unit, which investigates attacks, responded to a combined 761 data breaches, up from 141 in 2009. Of those, 482, or 63%, were at companies with 100 employees or fewer. Visa Inc. estimates about 95% of the credit-card data breaches it discovers are on its smallest business customers.

Hacking at small businesses "is a prolific problem," says Dean Kinsman, a special agent in the Federal Bureau of Investigation's cyber division, which has more than 400 active investigations into these crimes. "It's going to get much worse before it gets better."

Hackers are expanding their sites beyond big companies to include any business that stores data in electronic form. For small businesses, the impact could be crippling. Geoffrey Fowler reports for the Wall Street Journal.

In the time it takes to break into a major company like Citigroup Inc., a hacker could steal data from dozens of small businesses and not get detected, says Bryce Case Jr., a former hacker who broke into several government and corporate websites a decade ago and now runs an online message board for hackers called Digital Gangster. Now that small companies use computers, "the juice has become worth the squeeze," he says. "Even a pizza place has addresses, names and credit-card information."

Mr. Case, now a consultant in Colorado Springs, Colo., who helps small businesses identify security problems, has a trick for showing clients just how weak their systems are. He sometimes calls employees pretending to be a tech-department worker or consultant doing work for the boss and convinces them to tell him their passwords. "All you have to do is get a hold of one not-so-competent person and you're in," he says.



The fact that there are so many types of security threats makes it difficult for small firms to protect themselves. In April, the FBI issued an alert about a style of attack in which hackers steal a business's online banking login details and use them to transfer funds out of the business's account. That's what happened to Lease Duckwall just after 1 p.m. on Nov. 2, when someone logged into his company's bank account for Green Ford Sales Inc. in Abilene, Kan. The hacker added nine new employees to the car dealership's payroll and transferred $63,000 to them.

Mr. Duckwall learned about the transfers at 7:45 a.m. the next day. He called his bank, which froze the funds in six cases. But three payments had already been withdrawn by the recipients and the cash wired offshore.

"I don't have a clue" how or why his company was targeted, says Mr. Duckwall, who is still out about $22,000.

The costs of a breach can put a small company out of business. In 2006 and 2007, a Bellingham, Wash., restaurant called Burger Me LLC had its computerized cash register hacked. Criminals made untold numbers of fraudulent charges on customer credit cards.

After the incident, a credit-card company shut down Burger Me's account and put a hold on thousands of dollars in incoming payments, says Rich Griffith, its former owner. By late 2008, fees and lost business from not being able to accept credit cards put Mr. Griffith in so much debt—$12,000 for investigation and remediation costs alone—that he closed his formerly break-even burger joint

The cyber attack "cost me my dream," says Mr. Griffith, 47 years old. The hacker who stole the data was never identified.

Financially motivated attacks typically rely on computer code that hackers plant on victims' computers, often as attachments or links in emails sent to employees. While these malicious programs are well known to security experts, hackers tweak them frequently enough to render them undetectable to antivirus software.

Bigger companies, while not immune, generally do a better job of protecting themselves. AT&T Inc., for example, has a command center with giant screens that track all the traffic on its network. Other large companies mine data for warning signs, taking note when an employee swipes an identity badge in New York only to log onto the network from California, for instance.

Smaller companies are less likely to grasp the security threat. A 2010 survey by the National Retail Federation and First Data Corp. of small- and medium-size retailers in the U.S. found that 64% believed their businesses weren't vulnerable to card data theft and only 49% had assessed their security safeguards.

One of the most common styles of attack on small businesses targets credit-card information that a hacker can sell or use to make fraudulent purchases. To gird against this, the major credit-card companies in 2006 formed an industry group called the Payment Card Industry Security Standards Council, which establishes minimum technical protections for businesses that accept credit cards.

While credit-card companies require all businesses that accept their cards to comply with those standards, known as PCI, they have few measures to enforce them for small businesses. Bob Russo, general manager of the PCI Council, says many small businesses neglect basic security measures such as changing default passwords.

Mr. Angelastri's case shows how even a business that tries to protect itself can fall victim to hackers.

A Chicago native, Mr. Angelastri, 52, started his company in 1978 when he bought out the small street corner newsstand he started working at after high school. Over the years, he grew his business to two 1,500-square-foot locations in Chicago and Evanston, Ill., carrying more than 5,000 different magazines.

City Newsstand didn't have a computer technician on staff. But Mr. Angelastri had decades of experience with computers after converting to a computer-based cash register in 1990. That first computerized register, known as a point-of-sale, or POS, system, wasn't hooked into the Internet. Every time it needed to process a credit card, it would use a telephone modem to log into the bank.

Four years ago, he upgraded to a now-standard Microsoft Corp. Windows PC that connected directly to the Internet. Mr. Angelastri didn't ignore security. He regularly updated the payment software on his computer to keep up with the latest standards. About two years ago, he got a local technology contractor to install a payment processing system called PC Charge, made by VeriFone Systems Inc.

On April 14, 2010, he received an email from Accelerated Payment Technologies Inc.'s X-Charge, a sales agent for his credit-card processor, saying MasterCard had identified "some sort of breach or compromise" within his system. It didn't specify what, and asked him to fill out a questionnaire and return it within two weeks.

Mr. Angelastri checked his systems and called in an outside technology consultant. That investigator found one problem on his computer—a piece of hacking software known as malware—which the investigator removed. Still, X-Charge kept forwarding him emails between MasterCard and a payment processor called Global Payments Inc. that suspected fraud.

After a sixth email warning in June 2010, Mr. Angelastri says MasterCard demanded he hire a forensic investigator to do a thorough review of his system, essentially a digital version of the investigations that police often conduct at crime scenes. Mr. Angelastri hired Chicago-based Trustwave Inc.

A Trustwave investigator worked at Mr. Angelastri's newsstand until 2 a.m. one morning looking for cyber clues as to how his system might be leaking credit cards to hackers.

The investigator discovered a program called Kameo was capturing everything that came into Mr. Angelastri's system before it even reached the PC Charge payment software. Kameo was exporting that information over the Internet, giving hackers credit-card numbers, customer names and other details.

It turned out the hackers had been lurking in his system since April 15, 2009. They had gained access to Mr. Angelastri's computer through a program he used to periodically access his technology system from outside the shop. The program could be used by anyone who knew the password, and he had picked an especially weak one: "pos," a common nickname for the cash-register software that was also the system's user name.

Bob Cortopassi, Accelerated Payment Technologies' compliance security officer, said the breach happened because of a "lack of basic security requirements" and isn't the fault of its payment system. MasterCard declined comment on Mr. Angelastri's case, and Global Payments declined to comment.

Security experts say hackers routinely scan the Internet for computers configured this way. Such searches are fast and easy, and often the computers they find have weak passwords.

The hack on Mr. Angelastri's newsstand highlights another murky area of cyber attacks. The people whose information is stolen often are never informed, despite varying state laws that require breached organizations to notify them.

Small businesses like City Newsstand don't typically record the names and contact information of their customers and payment-card companies discourage businesses from keeping credit-card data. Mr. Angelastri never learned exactly which of his customers were affected, or how many.

Many small businesses complain they get little support from law enforcement or the credit-card industry once they are hit. After the investigation, Mr. Angelastri sent the report back to his credit-card processing company. It demanded he improve his technology, including installing a new higher-grade firewall. He also cut off access to the open Internet for the computers with the cash

register software. Now all they can do is pass information to the credit-card processor.

Mr. Angelastri says he is still paying off the $22,000 he spent on the investigations and security improvements. City Newsstand has thin margins, he says, on about $1 million in annual sales.

He reported the incident to the Chicago and Evanston police, but he never followed up. A spokesman for the Evanston Police Department said the department only has jurisdiction to look into crimes committed in the city, which it defines based on where the hacker is located. The Chicago Police Department didn't respond to a request for comment.

Mr. Angelastri also spoke a few times with the Secret Service, the federal entity charged with investigating hacking attacks, but he says that investigation didn't go anywhere. The Secret Service declined to comment.

Mr. Angelastri still doesn't know who attacked his system, but the hackers left some clues. Trustwave's investigation found that a Yahoo email address was receiving the data being collected by the hacker's malware. A message sent to that address by The Wall Street Journal wasn't returned. Yahoo said it doesn't comment on individual account holders.

The data also was being sent to an Internet server in Russia hosted by a Russian hosting company called FirstVDS, according to the investigation.

Aleksandr Belykh, the head of the abuse department of FirstVDS, said the user of the virtual server identified in the City Newsstand investigation is Russian, and his firm hadn't received any complaints about it. The company shut the account down in June after its owner failed to pay the bill. Mr. Belykh wouldn't disclose other details.

Mr. Angelastri still marvels that his business was attacked at all. "We thought there would be very little chance that somebody would come into a business of our size to pull off something like this," he says.

—Nonna Fomenko contributed to this article.

---

is now a Member of the Greater Victoria Chamber of Commerce!!

UPCOMING EVENTS

If you are in the Victoria area, why not check out

Speed Networking

Tuesday, October 18, 5:00 - 7:30 p.m.
Sponsored by: Art Gallery of Greater Victoria and Truffles Catering

Don't have time to waste and want to make new business contacts, check it out!

CRHNet Symposium

The CRHNet is a not-for-profit organization that was established in 2003 in response to a growing demand to promote and strengthen disaster risk reduction and emergency management in Canada.

October 19th to 21st, Ottawa Ontario.
Visit http://www.crhnet.ca/index.htm to register

24th Annual Emergency Preparedness Conference Nov. 29, 30 & Dec. 01

Emerging Trends and Challenges in Emergency Management

Register on-line at www.epconference.ca or email epconference@vancouver.ca

Welcome New members!

Remi Deveau, Sentry Partners Inc.

Stephen Anderson, BC Transit

John Gabel, Commisionaires Victoria

Having an EPICC membership can be very beneficial to your business. You will receive a copy of our monthly newsletter. You will have access to a large network of individuals and businesses in the Emergency Planning Industry. You will receive discounts on Seminars and Emergency Management Conferences.

We are always available to assist you, and if you have any questions please don't hesitate to **contact us 604-813-7979. www.epicc.org.**

DONT FORGET TO REGISTER FOR THE SHAKEOUT BC.
EPICC IS PARTICIPATING AND SO SHOULD YOU!!
Visit www.shakeoutbc.ca for more information

EPICC
147 East 14th Street, 2nd Floor
North Vancouver, BC V7L 2N4
Ph: (604) 813-7979
Email: info@epicc.org Website: www.epicc.org