CURIE

New FM Global Risk Reports

**by Gregory Gribbon*

What's inside

FM Global, one of the primary insurance companies providing property insurance coverage for CURIE's university campuses, is also a provider of property risk control engineering services. FM Global has been conducting risk control surveys of campuses since 1997. As of 2003, they have begun issuing (what used to be called their Loss Prevention Reports) their new Risk Report. The purpose of the new Risk Report format is to engender an improved risk management perspective and a more complete understanding of the hazards commonly found on campuses leading to better, more effective decisions and reduced losses. It builds upon the predecessor LPR's strengths, but also introduces new features and benefits that will increase its value and relevance to today's risk professionals.

The changes are more than just cosmetic. Improvements have been made to the underlying survey protocols and systems. Risk Report is the product of FM Global's "Exposure Driven Engineering" mindset that focuses attention on the factors that have driven actual loss experience for each type of risk or occupancy. Risk Report helps clients to:

- More readily understand the hazards and associated operational risks.
- Get the information universities depend on more quickly.
- Distinguish what is important from what is not.
- Know the options and make wiser, more practical loss control decisions.
- Form objective comparisons of risk quality within a campus and with other universities across the industry.
- Access relevant information that supports risk management decisions.
- Achieve sound, practical loss prevention solutions.

Risk Report takes full advantage of computer based technology, allowing for a format that is flexible and modular. The new report incorporates color graphics and digital pictures, where appropriate, to provide a clearer view of risk. The advanced platform allows FM Global to deliver reports quickly through FM Connect, FM Global's secure extranet - or they can continue to be received via e-mail. If you wish to subscribe to FM Connect, you can sign up on-line at www.fmglobal.com. Just have your account number and index number available. Contact Lisa Luksa, FM Global, Toronto (905-763-5617) if you cannot find your index number. Both numbers can be found on your latest Loss Prevention Report, or the newer Risk Report.

FM Global welcomes feedback on the report. If you have any questions feel free to contact *Greg Gribbon, FM Global Account Engineer (905-763-5611). ■

The Anatomy of a Slip and Fall

*by Stewart Roberts

Background: This loss happened on Sunday December 10, 1995 at about 7:30AM. The plaintiff is a 50+ year old male, custodial worker for the student federation who was leaving work after the night shift. He had departed the building, walked down a short sidewalk then out onto a driveway. He had walked nearly 25 feet from the building and had noticed a light dusting of snow on the ground. Walking at a normal pace, his feet slipped out from under him and he landed on his side. He had slipped on a patch of ice, which was covered by freshly fallen snow. There were two witnesses to this accident who confirmed the details. The evidence indicated there was sand under the ice. (note – it is believed that a bus for the band that played in the Student Centre that night, was left running and the warm exhaust caused the ice to form. It then snowed lightly.)

The University had sanded the roadway in question on Friday the 8th. Weather records show that 3.5 cm. of snow fell on the 6th and .8cm on the 7th. Overnight from the 9th into the morning of the 10th another 2cm.fell. No snow clearing operations were done. It was the University's policy to have regular snow and ice maintenance in effect during the week only. On the weekend snow and ice removal was done when complaints were received about specific areas. The specific area would then be dealt with.

The plaintiff suffered injuries to his lower back. He sustained soft tissue injuries a well as a prolapsed disc. He had some prior medical conditions including a shoulder injury referred to as frozen shoulder. This was not attributable to this incident. The plaintiff applied for Worker's Compensation benefits but his claim was denied. So was the appeal. It was deemed he was no longer on his employer's property (being the student federation) but rather the University's property and as his employer had no control over the area, they could not consider him for benefits. Although the plaintiff is now of retirement age he only worked for a few days following the accident and was then unable to return to work because of his injuries.

The Issues: Liability was an issue. The extent to which the injuries from this incident precluded the plaintiff from working again was an issue. A pre-trial conference was held with one of the presiding judges from the jurisdiction in which this matter would be heard. (Not the judge who would have done the trial). A trial date had actually been set.

The Occupiers Liability Act maintains that the occupier of a premises has a duty to provide a reasonable level of safety for users of the premises. As the student's centre is used on the weekend with fairly heavy traffic, it was suggested that there may be a greater duty for the University to have some sort of regular maintenance on the weekend rather than just the specific/complaint oriented maintenance.

The pre-trial judge suggested there was an exposure on the University, but the plaintiff also had a duty to look out and suggested it could go either way in court, but felt a 50/50 split would be fair. The judge also felt the entire wage loss was not a result of the fall, only part of it was. The plaintiff's demand was in the $500,000.00 range and we were able to

*** Stewart Roberts is the Claims Manager at CURIE.**

get this settled for $80,000.00 all inclusive. Adjusting and legal fees were another $23,500.00.

As you can see, the issues to keep in mind are: **What sort of maintenance procedures are in place for snow and ice removal and especially for after hours and weekends? What might the Worker's Compensation Board determine about someone else's employees on your campus? Are you keeping your campus at a reasonable level of safety**? The University had kept good records and were able to show the sanding had been done, even though this loss was not reported until May of 1996.■

Caveat Emptor: Wireless LAN Devices

This article was reprinted with permission from Marsh Risk Bulletin, February 2003.

According to networking leader Cisco, more than 10% of all U.S. organization with 100 or more employees have either piloted or implemented the use of Wireless LAN technologies (WLAN) within their organizations. Organizations that are pushing forward must be aware of the various vulnerabilities and risks involved with this emerging technology in order to proceed wisely.

Given the broad-spectrum distribution methodology of any wireless device, one must initially examine one's assumption that physical security is the first line of defense. **802.11b,** the IEEE's emerging standard of wireless LAN based connectivity has a basic 300-foot distribution transmission/reception perimeter that is circular in nature. Add to this base ability, the widespread use and availability of signal boosters and/or directional antennae, the general assumption of perimeter "good fences make good neighbours" defense needs to be reconsidered. In other words, multi-dimensional and multi-directional signal leakage points must be contemplated when placing/employing all devices.

Another unique risk consideration to Wireless LAN devices is the widespread knowledge of 802.11b's relative weaknesses. As with other emerging technologies in recent memory, the **Internet Age** has created a wide consortium for the publishing of known 802.11b flaws and exploits. The low modicum of technical sophistication required and/or perceived limited "risk of capture" has lead to a culture of so-called "drive-by hackers". Scanning and attack kits are developing as quickly (if not faster) than the actual engineered standard.

Yet, the most significant security consideration with the use of wireless LAN devices during experimentation is network segmentation.

Wireless LAN devices are exceptionally vulnerable to:

- **Broadcast Monitoring:** Due to WLAN's broadcast nature, location and isolation of transmitting devices are easily discovered and thus monitored.
- **Unauthorized Access:** Once a transmitting device is discovered, an intruder sniffs for device or community transmission membership groups codes and thus access is gained.
- **Masquerading:** Further packet analysis allows for the capture of individual User ID's and passwords. The intruder then inherits all the rights and resource access accorded to said user.
- **Bandwidth Siphoning:** In many cases, attackers will simply exploit the commodity of bandwidth available to the network. But the utilization of so-called "free bandwidth" also opens up the risk of company resources (storage space, IP hijacking) being used for "attack

anonymity" which may have consequential risk such as remote toolkit deployment, legal accountability and/or improper logging.

- **Denial of Service:** Intruders have been known to congest resources to create business interruption.

As such, wireless LAN devices should be segmented from internal networks and/or sensitive digital assets as if they represented the same threat as a completely public connection.

In terms of risk mitigation, IT departments have to begin creating hardening procedures and diligently administer the configuration of devices. For example, wireless devices are shipped with a default configuration that emphasizes ease of installation with well-know default settings. One should, at a minimum:

- Change the default Server Set ID (SSID)
- Enable Wired Equivalent Privacy (WEP) to 128 bit encryption at a minimum [1]
- Change the SNMP community words
- Modify interface defaults to unique values
- Protect client-based registry settings

Most industry analysts feel that the global market for WLAN technologies will continue to increase at a 25% percent rate with enterprises becoming the leading consumer by 2005. The increases in productivity due to roaming and decreased cabling costs will, no doubt, drive adoption rates in the future. Yet, failure to create proper controls could result in reputational/performance impacts and, in the worst case scenario, material impact on organizational value. Organizations should begin considering **formalized IT risk assessments** that result in policies surrounding the appropriate use of wireless technologies and procedures that monitor for unauthorized devices.■

[1]WEP Encryption has much to be desired in terms of strength at this point in time, it should only be considered as mild deterrent to the skilled intruders. 802.11g, which is not expected to become a ratified standard until Q3 2003 should address this issue.

DATES TO MARK ON YOUR CALENDAR

October 18 -19, 2003 **CURIE University & College Risk Management Conference (AGM)**
Grand Pacific Hotel, Victoria, BC

October 19 - 22, 2003 **CRIMS Conference**
Victoria, BC

CURIE FALL REGIONAL RISK MANAGEMENT WORKSHOPS

Western Region	Ontario	Eastern Region
Saskatoon, SK	To be announced	Halifax, NS
		November 18 & 19/03

CURIE Risk Management Newsletter
Published and distributed by Canadian Universities Reciprocal Insurance Exchange (C.U.R.I.E.), 5500 North Service Rd., 9th Floor, Burlington, ON L7L 6W6
ISSN 1196-085X
Telephone: (905)336-3366 Fax: (905)336-3373 Editor: Keith Shakespeare