**Dustin Biernacki**
dutz_bier@hotmail.com
University of Melbourne

# The digital world of risk

The world of cyber attacks is becoming increasingly familiar to financial institutions and likewise to those in the actuarial profession. It's apparent that pricing this type of risk is not performed to the same degree of self-assurance as the more mainstream insurance lines.

Rampant growth of the digital world only adds to the complexity and dimensions to any risk factors worth considering. Constant changes in software, platforms and other interfaces mean that much of the risk is shaped by the way which the security of these interfaces is designed and updated on a regular basis.

So, if I were a CEO, what sort of digital dangers would I be concerned that my company was facing these days? I believe there are a great number of these risks to be considered, but I've attempted to distil them into five categories:

1. **Data destruction**, deliberately or carelessly causing important information to be lost.
2. **Theft/extortion, stealing** any amount of funds. This could also include stealing services such as impostor wireless networks or presenting as a major firm with the intention of unlawful gain.
3. Third party **losses due to errors/omissions** made by the providing company, which presents itself with liability issues.
4. Physical **cyber terrorism,** involving a terrorist entering the building and gaining access to the control room.
5. **Vulnerability to printing errors** when programs are crashed. If error messages print successfully when hackers stretch the limits of an application, it could provide an insight as to any weakness of the application. These weaknesses can be used for exploitation.

Mobile phones add yet another aspect to this issue. According to the 2011 Georgia Tech Cyber Security Summit (GTCSS), there are over four billion mobile handsets in use around the world. Usage levels of mobile browsers are set to exceed desktops by 2014. Due to higher level of underdevelopment in mobile software systems, they have become a suitable target for a variety of hackers with various skills. Previously limited to computers, and arguably targeted towards Windows / Internet Explorer - smartphones are now at the top of this list.

Potential for 'spreadability' is also monumental when you consider how vast the mobile network is and how many methods of communication the latest smartphone actually has. There is SMS, MMS, internet browsers, email, Facebook, Skype, contact lists, voicemail and more. That's more than enough platforms to choose from as far as an attack is concerned.

One major disadvantage of these devices is that the software/operating system is not updated regularly by the user. This gives the attackers an upper hand, as they know exactly what can go wrong on older operating systems. Another concern raised by the GTCSS is the rapid growth in mobile applications.

Just like in the insurance world, development teams are under pressure to come up with products quickly. This is good for overall satisfaction of users, but may not be as optimal when it comes to security. Time constraints in which the development occurs will limit how rigorously the data is validated.

This isn't just limited to phones either, with systems, processes and storage within companies often lagging behind the product development itself. This creates pockets of vulnerability that can be exploited.

When considering exploitation, we should not omit the controversy surrounding Rupert Murdoch and the celebrity phone hacking scandal. The question is not so much what the purpose was of such activity, rather how did it happen so easily and how easily could this extend to corporate espionage?

Several years ago mobile phones were far more primitive than they were now. Allegedly, the method of hacking used for these devices was SQL injection, a rather superficial but deadly form of attack if used properly. With ease of access to confidential information on the subject of celebrities including the royal family, one may realise why it may have been so tempting.

There is a third world war, and it is a cold war in the digital era. Managing risk has a new test in this age and we will have many challenges and interesting times ahead of us. This type of risk must be brought to the fore and be understood in far greater detail. The protection of your personal information is at stake. A