Dawn Simmons
Senior Underwriter, International Professional

XL Group
Insurance
Reinsurance

Cyber Liability

The Dark Side of Technology – the evolution of cyber crime

"Powerful you have become, the dark side I sense in you." – Yoda, Star Wars

While Yoda appeared on screen back in the 1980s, his quote has relevance to today's technology. The advent of technology in the last decade has been immense. And while technology has already brought many beneficial changes, it can be argued that it also has a dark side – that of cyber crime.

We already have our very own modern day attackers which include hackers, spies, terrorists, corporate raiders, professional criminals, vandals and voyeurs. This type of "cyber warfare" exploits vulnerabilities across networks. Recent examples include the high-profile hacking of Sony's PlayStation Network which has brought the dangers and costs of hacker attack back into the spotlight. The reported theft of personal – and possibly also credit card – information of up to 100 million customers world-wide certainly makes this one of the largest ever data heists, with the full financial impact not yet known. Sony estimates that the hacking will cost it around $170 million this year, but some experts predict this number to be significantly higher, especially as more details about the extent of the attack are still emerging.

And the way we connect has changed rapidly. According to the World Economics Forum Risk Report 2012 about 470 million smartphones had been sold worldwide and this number is projected to double by 2015[1]. And the number of Internet-connected devices is predicted to exceed 15 billion – twice the world's population – by 2015, and to soar to 50 billion devices by 2020[2]. Currently there are five billion devices or "things" connected and remotely accessed from the internet[2]. "Devices" of course refers to more than smart phones, netbooks and tablets. It also refers to systems such as smart grids, intelligent transportation, healthcare monitoring, smart manufacturing, and environmental sensors.

While technology continues to advance incredibly quickly, many organisations and individuals have been slow to recognise the inherent cyber risks connected to this technology. For example, the European Commission has finally got around to fully updating their EU Data Protective Directive from its original introduction in 1995. The new directive includes proposals to introduce a single set of rules on data protection, valid across the EU and means companies and organisations should notify the national supervisory authority of serious data breaches within 24 hours wherever possible. For the company of the future, technology will be the major enabling force for business in the future trans-forming supply chains, value nets, business models, and workstyles and opening up new global markets for expansion.

So how big is the threat of cyber crime and how will this threaten organisations in the future?

There is no doubt that societal behaviour is being shaped by our activities in cyberspace and the future of technology is almost impossible to predict. The arrival of cloud computing has been embraced by many organisations (including the New York Stock Exchange (NYSE)). Cloud computing enables organisations to outsource storage and applications to distant servers, and it is widely expected that the adoption of cloud technology won't just continue, but accelerate. But storing data in a cloud setting brings its own set of inherent risks. Often there are "multi-tenants" storing data in the same cloud space. This means that a data breach or hack intended for one company may result in many organisations data being breached. This can be seen in the recent data breach suffered by Epsilon – the world's largest provider of permission-based email marketing with one of the biggest customer databases – a key target for hackers. Hackers caused a data breach which may have swiped customer data belonging to the world's biggest brands and has dented the image of cloud technology. Nevertheless, the limitation of hardware means that virtual data storage will continue to advance.

Additionally, it is expected that our computers will become ever more powerful. The Moores Law theory outlines the trend in computer processing power which has been increasing exponentially for over a century. Will artificial intelligence become the norm? Can we envisage a situation where computer technology is so powerful that many high-level tasks in business and government are being handed over directly to them? Many think so. It is not just the design of the computer (hardware) but the software that will advance. For years, software had lagged behind hardware in development, which impeded the spread of artificial intelligence, but this is no longer the case. Ever more sophisticated programs and apps are continually improved. This, in turn, could lead to an "intelligence explosion", with some of the biggest political decisions on the world stage being eventually influenced by sentient machines.

For the company of the future the technology is likely to be supported by artificial intelligence with "virtual" data storage. It is expected that more and more sophisticated social networking will be driving consumer choice.

This increasing reliance on technology means that organisations must be must be proactive instead of reactive when assessing technology risk. As good practice, companies that manage risk proactively should implement crisis response procedures for responding to any data breach. Having no, or a poorly implemented, crisis response plan can cause nearly as much damage to the brand as the breach itself. The 24 hour news media wants to be fed with immediate answers and solutions. This 'feeding frenzy' is increasing ever faster, as news and views travel across market and national boundaries via social networking sites, requiring a whole new level of

communication across continents and languages.

So what does all this mean for firms wanting to protect themselves? The growing threats and potential costs outlined above mean companies need to constantly assess their exposure to cyber risks and their own security measures. The overall impact and cost is not only determined by the data breach itself, but also the handling of the immediate aftermath of post-data breach to help reduce the longer-term impact and costs of a hacker attack. Many are turning to insurers for a risk transfer solution to help mitigate this exposure. While cyber liability insurance has been around in some form or another for the last decade, the never-ending advances in technology and resulting regulation to try and control it means that organizations will have to put cyber protection measures in place. As a result, insurers have expanded the insurance protection to offer not only coverage for the ensuing liability, but also for costs related to reputational management, business interruption, data breach notification and/ or credit monitoring, as well as regulatory fines. Companies will need to select their coverage requirements depending on the nature of their business and the breadth of information which they are legally obliged to safeguard.

The future of technology is uncertain. All we can know is that today's tablets, iPads and clouds will be superseded by the next generation of connectivity – but all advancement can bring new challenges and it is important that we are all – companies, organizations and individuals – ready to manage that risk.

[1] *Nagamine K. "Worldwide Smart phone Market Expected to Grow 55% in 2011 and Approach Shipments of One Billion in 2015" International Data Corporation*

[2] *World Economic Forum Global Risks 2012*