CAPTIVA
INSURANCE MANAGERS

REPORT

Cyber Risk

The new risk on the block is Cyber Crime.

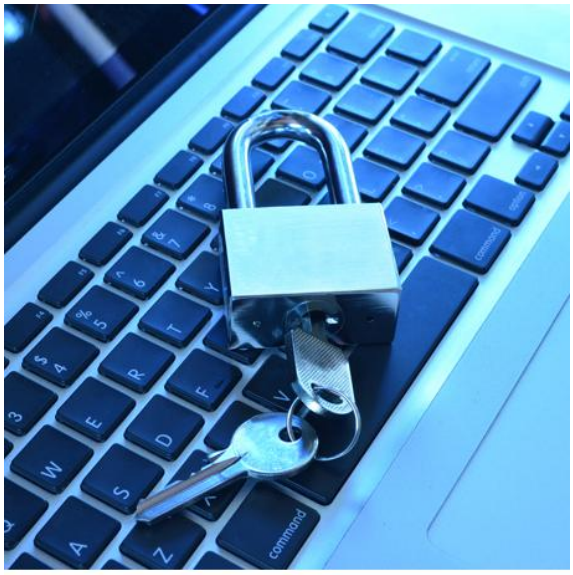
Despite the enormous amount of media coverage that cyber crime is getting at the moment, it is amazing that so few senior company executives are taking it seriously. Unfortunately, unless they prepare themselves soon, it may be too late.

The press

Cyber security is grabbing the headlines, and it is easy to see why. Just type in "cyber crime" to your PC and you'll see for yourself what's going on. The figures are startling. Reports indicate that cyber crime costs the UK economy up to £27bn each year, with the worldwide annual cost reaching around $388bn (£253bn). As mobile devices proliferate and cloud computing continues to develop, the threat presented by the hackers grows ever more acute.(1)

In 2010 the number of devices connected to the internet stood at around 12.5 billion. Experts advise that this will grow to roughly 25 billion in 2015 and 50 billion by 2020, providing more fertile ground for cyber criminals.(2)

Every day customers are being asked to reset passwords. In 2012, 50 million users of a well known social media site had to do this after hackers had attacked the company's servers and potentially made off with personal data. The cyber attack resulted in access to customer data including names, email addresses, dates of birth and encrypted passwords.



Although the majority of cyber crimes are financially motivated and aimed at large well known targets, one in five is cyber espionage. This type of attack is designed to cause disruption and/or to steal valuable intellectual property.(3)

Recent reports have found that the net loss due to cyber crime now outweighs the global narcotics trade. Today, cyber crime costs more than $1.0 trillion to society, with billions of dollars being stolen from small, medium and large-sized enterprises.

While most people would correctly conclude that financial services operations represent the highest target industry segment for cyber issues, many would be surprised to know that health care is the second most popular target. In fact, data obtained from health care-related organisations is the most prized type of information a hacker can obtain.

There are many reasons why companies are attacked by cyber criminals. It could be for financial gain by having access to other

people's credit card details, it could be industrial espionage where one company wants to seriously disrupt the business or reputation of a competitor, it could be to steal confidential design plans, or it could be a slur campaign against a particular company or institution. And, as we know from reported incidents from China, it could be for political reasons.[4]

Attitudes

Although we appear to be aware of the huge risk of cyber crime, the risk management and insurance industries do not seem to have placed it as a priority yet. This can clearly be seen from the biannual, Aon Global Risk Management Survey, which lists the top 10 risks facing organisations today, and what they think they'll be in 2016:

Risk Description	Risk Rank	Risk Rank
	2013	2016
Economic slowdown/slow recovery	1	1
Regulatory/legislative changes	2	2
Increasing competition	3	3
Damage to reputation/brand	4	8
Failure to attract or retain top talent	5	5
Failure to innovate/meet customer needs	6	4
Business interruption	7	11
Commodity price risk	8	7
Cash flow/liquidity risk	9	10
Political risk/uncertainties	10	6
Weather/natural disasters	16	9
Computer crimes/hacking/viruses etc	19	

I have added two risks to the end of the list to give an idea of how risky they are perceived to be in comparison with the top ten. I'd like to draw your particular attention to Computer crimes at the bottom, which is rated only number 19. Many experts believe that cyber crime is about to change the whole world of risk management, and is the new big risk. I believe that by 2016, cyber crime will be comfortably in the top ten, and that those companies that are not prepared for it will have difficulty surviving.

Other research conducted in association with Federation of European Risk Management Associations by Harvard Business Review Analytic Services, Zurich and others is not any more encouraging. That research shows that many companies still do not devote sufficient attention to cyber risks. Apparently only 16% of companies have appointed anyone to oversee cyber risk, and fewer than half (49%) agree that they have a strategy for communication to the general public in case of a cyber risk incident.

Probably most surprising is that only 19% of respondents have purchased security and privacy insurance specifically designed to cover exposures associated with information security and privacy issues.

The scary thing is that although the directors of a number of high-profile businesses have started asking their executive teams to implement systems to avoid the risk, it's probably already too late, the hacking has already started.

Insurance

A number of insurance companies have recognised that the insurance of cyber risk is a new marketing opportunity, and have designed new products. However, the wordings vary considerably, but ideally the policy should include cover of:

- Damages claimed by third parties for network security breach
- Costs incurred to notify persons impacted by data breach
- Regulatory fines imposed by governments (if possible)
- Costs to restore data lost or compromised
- Investigation costs for computer forensic analyses
- Crisis management costs – public relations and damage control
- Coverage for losses to or caused by your data that's maintained by a third party
- Coverages for 'gaps' in typical general liability policies for claims arising out of the creation and distribution of content on websites, blogs or social media.

Although competitive premium rates may still be available to encourage potential insureds to transfer their cyber risks, one wonders how long it will be before the cyber claims need to be paid and the rates shoot up.

Captives

Due to the fact that much of the traditional insurance market has yet to develop modern and suitable policy wordings, and to avoid the real risk of fluctuating premiums, the obvious solution is to utilise a captive insurance company. The captive can make[1.] sure that full protection exists and that there[2.] are no gaps in coverage. There are many other benefits of having a captive involved, not least of which is that if the risk management policy of the parent company is successful, the profits made in the captive can be invested back into the risk management process, i.e. the captive can be used as a profit centre.

Due to the possible high sums insured and limits of indemnity of insuring cyber risks, it is unlikely that a captive would be able to insure the whole risk, but one of its many advantages is that it is a flexible risk financing vehicle. Captive owners may wish to consider using their current captive for deductible "buy downs" on their cyber coverage. As excess coverage is currently readily available, this may be a good time to establish a relationship with a well known and reputable underwriter. By using excess coverage, the captive can customise its primary coverage to meet specific needs and to fill any gaps in the traditional market offering.

Conclusion

Cyber risk is here to stay, and it is only a matter of time before it works its way towards the top of the list of risks which organisations face. The insurance industry is readying itself by developing new policy wordings and managing all sorts of new claims. The captive industry is also well placed to start adding cyber risk insurance to the suite of services it provides, which should be welcomed and encouraged by all regulators.

Conor Jennings,
Captiva Managers, Cayman Islands
c.jennings@captivamanagers.com

Source References

1. European Forum for Member States (EFMS)
http://www.pts.se/upload/Ovrigt/Internet/Branschinformation/rgig-kommissionens-forslag-european_strategy_internet_security.pdf

2. CISCO
http://share.cisco.com/internet-of-things.html

3. Living Social
http://www.networkworld.com/news/2013/042613-livingsocial-gets-hacked-50-million-269196.html

4.Narcotics
http://wck-grc.com/the-cyber-challenge/