



Olatunji Oluwatosin is tried for his role in the ChoicePoint identity theft case

AP

Cracking the hackers

Are re/insurers keeping pace with the ever morphing face of cyber risk asks **Tim Evershed**

Cyber attacks are a growing threat to industry and governments as they continue to multiply, evolve and grow in prominence.

Recent stories in the mainstream news underline this fact with, most recently, North and South Korea opening up another front in their hostilities, this time online as hackers from both sides used cyberspace to launch attacks.

Even more famously the WikiLeaks website embarrassed global governments with its revelations. In October 2010 it leaked details relating to the Iraq War, before in the next disclosure revealing thousands of confidential diplomatic cables.

WIKILEAKS LESSONS

As a result obtaining sufficient protection from data leaks and other types of attacks has become a priority issue for public and private sector alike.

Marcus Alldrick, Lloyd's senior information risk and protection manager says: "At the core of the Wikileaks issue is access rights. We have to ensure we learn to ensure that access rights are commensurate with peoples' roles. To do that would have been preventative action."

In the fallout from the WikiLeaks incident supporters of the whistle blowing website retaliated against firms including Visa, MasterCard and PayPal. They attempted to bring down their websites with denial of service attacks – these flood networks and stop them functioning.

Emily Freeman, executive director of technology, media and communications at Lockton says that such attacks are not a new phenomenon.

"These attacks can be used for a number of reasons, for terrorists looking to stop the sites, for extortion for commercial gain or simply individuals who just do this to show that they can."

According to Ms Freeman companies should view this issue as a battle that needs fighting around the clock, every day of the year. In order to fight the battle successfully companies will need to constantly examine their networks, constantly ask questions of their networks and continually upgrade them. They require a multi-layered defence against attack and a mitigation plan in case an attack succeeds.

Ms Freeman says: "It is being able to detect that your network is under attack and

THE BRIEF

- Wikileaks saga creates questions of access rights to information
- Constant surveillance required to guard against denial of service attacks
- Many attacks sparked by careless behavior with laptops
- Re/insurance rates becoming more consistent as market matures
- Public sector's risk profile raised as a result of constant attacks

having the ability to switch to an alternative network. You need a robust separate network able to take the traffic if the first network is brought down.”

“In terms of the denial of service attacks, it is a question of what are the contingencies companies have to keep themselves online?” says Mr Alldrick.

“There have been examples of companies that have successfully migrated their services to alternate sites. The trick there is letting your customers but not your attackers know what you’re doing and that requires excellent customer communications.”

However, denial of service attacks are just one of a range of possible attacks a company could face against its systems.

“The protection of personally identifiable data, particularly of a financial or healthcare nature is a big issue. Personal data that is not meant to be in the public domain and how do you protect that data?” says Ms Freeman.

REDUCING RISKS

“People can successfully break into the data by malicious codes or malware and pass it onto criminals who use it for identity theft. Companies need to apply patches to their systems, examine their logs regularly and run tests to see what your vulnerabilities are and use encryption for defence,” she adds.

As well as defending themselves from deliberate criminal attempts to compromise their data companies must also be aware of the potential damage caused by laptop theft or the loss of USB sticks that contain sensitive data.

David Hallstrom, property/casualty underwriting director at US insurer CNA says: “Over half of the breaches that we are seeing are through some physical loss of data. A lot of it boils down to human error – people leave laptops visible in their cars or papers can be left in hotels, cafes or somewhere else they shouldn’t be.

Although these losses are largely attributable to human error or rogue employees, and therefore almost impossible to eliminate, there are measures that companies can take to reduce their risk, such as encrypting data.

Gareth Tangatt, underwriting manager for cyber liability at Barbican, says: “You generally find that US entities are ahead of the UK in data security and system protection. In the US most companies have encryption on their networks, laptops and even Blackberries. In the UK only a few large organisations have that, which leaves the rest open to attack.”

Mr Tangatt adds: “Legislation is becoming more in line with US data protection laws and a bill was passed in April 2010 giving the Data Commissioner powers to fine commercial organisations for data breaches.”

**Wikileaks:
what can the
saga teach re/
insurers about
cyber risk?**



PUBLIC SECTOR TARGETED?



The public sector was well aware of the risk it faced long before the WikiLeaks saga began as evidenced by a long list of incidents over the years and the UK’s decision last year to put the threat of an attack on computers at the

most serious level – ‘Tier 1’ – alongside acts of international terrorism or a military crisis.

Malcolm Randle, an underwriter in the enterprise risk division at Kiln, says: “Attacks on the public sector are regular. The Beijing Olympic Games saw the Games’ official website, plus a number of Chinese government websites, up against thousands of attacks on a daily basis. These were not necessarily aimed at stealing data, but to voice protest, deface government or police websites and embarrass those in positions of authority.”

But what can governments learn from industry? And does the insurance industry have a part to play in helping mitigate the threat to the public sector?

Mr Randle adds: “The public and private sectors have to work together because of the overlap created by our reliance on technology and the internet.

“The insurance industry could work with the public sector, provided the appropriate controls and protocols are demonstrated and adhered to. Unfortunately for the public sector it is a regular target for attacks, which would increase the risk’s profile,” he concludes.

According to cyber experts at CNA, the saga at ChoicePoint Inc, which became the centre of an identity theft scam was a watershed for firms finally realising what cyber liabilities they may be sitting on and caused many to turn to the insurance industry.

In 2005 the company another fraudster accessed 40 million credit card accounts at CardSystems Solutions.

The company not only had to pay over \$50m in a combination of fines, fees and other costs but ended up in front of a Congressional hearing.

Mark Silvestri, vice president of product development at CNA says: “Generally, demand is up too. On a percentage basis we are experiencing a double-digit increase in volume year over year. We are also seeing more demand from unregulated sectors.”

“Whereas regulated banks and healthcare companies sought coverage in the past, now we’re seeing increased demand from technology and professional firms. Even the manufacturing and construction segments are showing interest.”

“The best policies have actually evolved to reflect such changes in exposures,” adds Mr Silvestri.

Mr Tangatt says: “In terms of the capacity there is enough around to build towers of indemnity. The market in the last few years has been encouraging and we have seen rates become more consistent as the sector matures.”

According to underwriters the available capacity is enough to build \$250m global policies, while coverage of up to \$100m is obtainable in London.

“This has primarily been driven by the participating markets within the class, especially from within the London Market. In addition, many of the much anticipated legislative amendments have now come into force, so that claims and the consequential exposures can now be measured more accurately and quantifiable statistics gathered for comprehensive review by actuaries,” adds Mr Tangatt. 