Waging war in a technological age

A recent cyber attack linked to North Korea reveals that the hacking threat has reached new levels

IN 2012, US BUSINESSES LOST MORE THAN $1 trillion dollars worth of intellectual property owing to cyber attacks, according to the US government. Multiply that 100-fold to include other industrialised nations and the figure is astronomical. In the past few months, 15 of the largest US banks have been offline for a total of 249 hours, including Citibank, Wells Fargo, Chase and Bank of America. The latest high-profile attack on South Korea's top financial, media and military structure highlights the issue is not only a growing concern for businesses, but is now also enveloping entire nations. Further, and worryingly, the worst may be yet to come.

The South Korean attack begun as a war of words between South Korea, North Korea and Japan. Add to the mix North Korea's threats of nuclear war, and a point of escalation appears from which it would be difficult to return.

DAC Beachcroft partner Ken McKenzie says the cyber attack was mostly political, but it is difficult to identify the culprit. "The South Korean episode is believed to be political, a suspicion supported by the fact that, this time round, banks, utilities and broadcasters – important parts of the infrastructure – were denied access or had data scrambled in what are seen as a linked series of attacks.

"While North Korea is suspected of being the sponsor, many also believe that the activity and technical skills emanate from China. China hotly denies this, pointing out that the semblance of location is easily faked."

City University London professor of systems and cryptography David Stupples also believes the attack emanated from China but was ultimately successful because it was an insider job.

"I think it was done using insider information and using insiders to gather the worms and load them into the system. I believe there is a great deal of espionage going on in this situation because [the hackers] attacked so many organisations at once and so successfully as well. It was probably a joint effort with the Chinese government and a lot of insiders helping as well."

Worse to come

The event could have been worse, according to experts and risk managers. The South Korean episode lasted 10 days, but it is not hard to see that economic or even physical consequences could be dire if a national banking, utility, or aviation system were incapacitated indefinitely or, as has previously happened, if military IT were disabled.

Alamy

"One sobering view is that the South Korean attack was only a reconnaissance – if so, there could be worse to come," says McKenzie. "Another is that it was a tit-for-tat reprisal from the North or its supporters for a perceived similar move against [the North]; either way, the political climate of the region is of renewed and escalating hostility."

The single biggest issue for businesses and nations in the age of cyber warfare is keeping up to date with modern cyber terrorists. Not only is it difficult to be ahead or even to stay up to date with cyber crime, but to do so also costs businesses a fortune.

One European risk manager who asked not to be named told *StrategicRISK* that his company "spends millions of euros on security but we are continuously breached by hackers. It is hard to not think it is a pointless game."

Never-ending chase

Stupples says that even the top software firms are always one step behind cyber criminals and always trying to catch up in a dangerous game of cat and mouse.

"Once a virus has been detected, [businesses] can then develop the ways to combat that virus. But where do they test the new programme? They have to test it by sending it out to testers. Who are the testers? Some might be hackers themselves. So there is even leakage of malware software."

But it gets worse, says Stupples. "Hackers are already finding loopholes in the software before the company has even launched the product or we have implemented it. Therefore, hackers are actually preparing to attack the new software as it is being issued. It takes 100 to 140 days to issue updates to fix the issue. So from day zero to the day the anti-viral update comes out is the time in which cyber criminals can start earning money by doing damage to the systems."

Mitigating the risk is difficult in the event of cyber warfare as an imminent attack is possible from many different points. Insurance is one method of mitigation that is gaining momentum, experts say. Alarmingly, according to a recent survey by insurer QBE, 32% of UK companies still have no plan or protection in place in the event of a cyber attack. This is an improvement when compared with last year's figure of 46%. The survey showed that 94% of the financial sector was well prepared, but only 44% of the building and construction industry has a plan and a mere 25% has insurance.

"Awareness is growing and the insurance industry is up for it, but many businesses' understanding of the risk is still relatively unadvanced and struggling to keep up with the pace of change," says McKenzie.

Internal spies

Still, the biggest risk for any company comes from its employees. Stupples says: "Asking 'can they be bought?' is always a good starting point. Companies need to vet employees. I am sure they do that, but you can never get 100% loyalty because someone can always be bought.

"But more importantly, companies need to start structuring their systems to make it more difficult to steal intellectual property. They need to put in structures where no one person has knowledge or access to the whole system. Encrypt data and keep all viral and firewall systems up-to-date."

Even as this article is being written, hackers are targeting financial institutions and internet service providers in the US, the Netherlands and Israel. There seems to be no end in sight for businesses, so the best advice is to be as prepared as possible and always remain on top of systems updates. **SR**

Lowdown: cyber attack viruses

FLAME The most advanced and sophisticated attack tool on the market. It is 20 megabytes in size and is larger than other malware used. It is unique because it steals information, including recording audio, taking screen captures and transmitting visual data. It can steal information from the input boxes when they are hidden behind asterisks and password fields. Also, it can scan for locally visible Bluetooth devices.

STUXNET Discovered in 2010, it is believed to have been created by the US and Israel to attack Iran's nuclear facilities. Stuxnet initially spreads via Microsoft Windows and targets Siemens brand industrial software and equipment.

DUQU Discovered in 2011 and thought to be related to Stuxnet. In itself it is not a destructive virus, but collects internal data from industrial control systems that can be used in later attacks.

> *'One sobering view is that the South Korean attack was only a reconnaissance – if so, there could be worse to come'*
>
> **Ken McKenzie**
> DAC Beachcroft