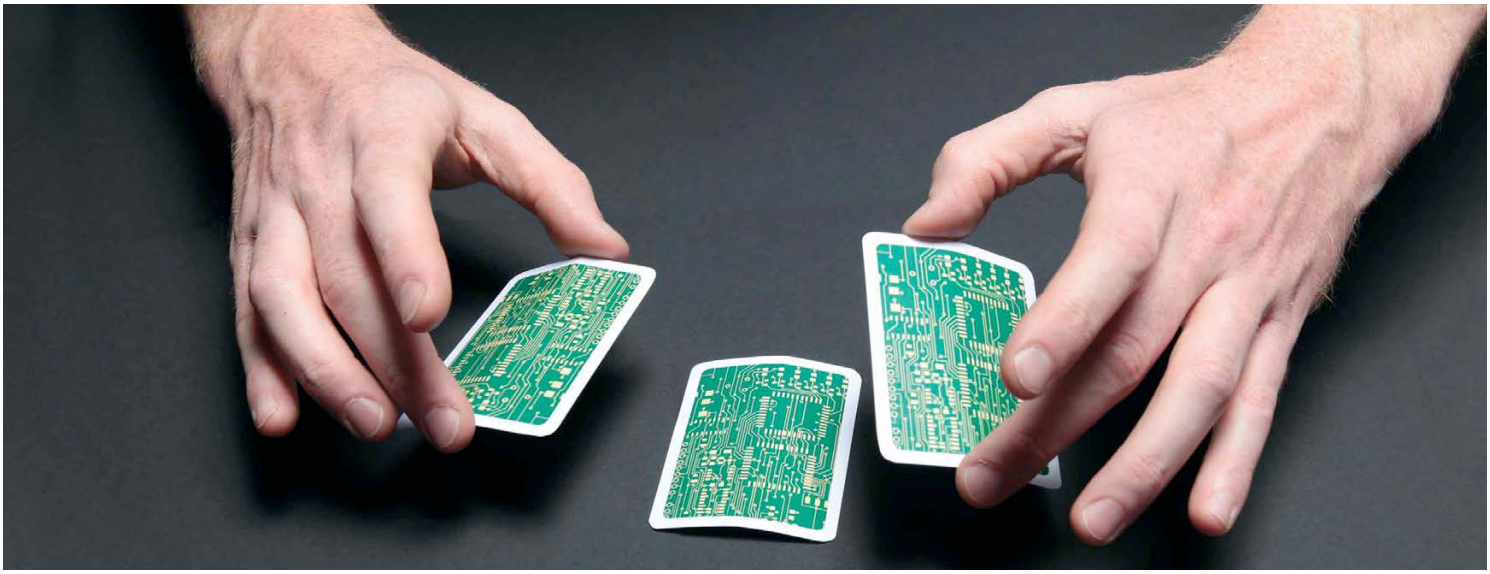
SLEIGHT OF HAND

Cybercrime is the 21st century's magic trick – but the risks are no illusion



Shortly after lunch (US time) on 23 April 2013, the Dow Jones crashed. In seconds, 1% was wiped off the market value of US stocks for no apparent reason.

Although the market recovered within a few minutes, the flash crash left many scratching their heads. It had been caused by a single rogue tweet posted from the Associated Press (AP) Twitter account by hackers, claiming that there had been explosions at the White House, and Barack Obama had been injured.

The carefully targeted hack (gaining access to a computer network) was just one of a series of high-profile cyber attacks to have taken place this year, with victims ranging from media outlets including AP and the Financial Times, to technology companies such as Apple and Microsoft. The concept of hacking isn't new – hackers have been targeting governments since the early 1990s, many for the kudos of cracking seemingly impregnable security software – but the nature of attacks has changed in recent years.

CHANGE IN MOTIVES

Today, states and companies have to contend with attacks from hacktivist groups, foreign governments and criminal gangs looking to steal sensitive information for financial gain. But just how big is the cybercrime problem, what are the main dangers that businesses need to be aware of, and what can technology companies, in particular, do to protect themselves?

HACKERS HAVE BEEN TARGETING GOVERNMENTS SINCE THE EARLY 1990S, MANY FOR THE KUDOS OF CRACKING SEEMINGLY IMPREGNABLE SECURITY SOFTWARE

The most recent data highlights the threat. According to the 2013 Information Security Breaches Survey, commissioned by the Department for Business, Innovation and Skills, 93% of large UK organisations (with a turnover of more than £5.75m or with more than 250 staff) and 87% of small firms were targeted by hackers in 2012 – an increase of 10% on the previous year. The average cost of a breach was in the region of £450,000 to £850,000 – enough to wipe out a small to medium-sized enterprise in one hit.

The situation is similarly grim in Ireland, with businesses reporting 15 attacks to IRISS-CERT, Ireland's voluntary computer emergency response team, in 2012, compared with just five the previous year.

As a result of current laws for the reporting of breaches in the UK and Ireland, there's a strong chance that these figures only tell half the story, according to Colin Tankard, Managing Director of data security company Digital Pathways. "How big the threat of cybercrime in the UK and Ireland has become is really an unknown, because, as in Europe, companies do not have to declare a breach," says Tankard. In other countries, including the US, there is a legal obligation to report such incidents. "Statistics from the US show, for every one reported incident in the UK and Ireland, there are over 200 there."

Tankard adds that technology companies are often targeted by hackers ›

because many of them hold data such as credit card details and intellectual property, plus they are a good source of new product developments that have a financial value. Technology companies know they're at risk, but this knowledge doesn't make it any easier for them to combat the threat, says cyber security expert Ross Anderson. "I'm afraid there's no silver bullet," he says. "Anti-virus software doesn't work very well, as those who write malware test it to ensure it's not detected. The tax money spent on GCHQ [Government Communications Headquarters] doesn't help businesses as the spooks just worry about other governments. Businesses just have to educate themselves on the risks."

PROTECTION AND PLANNING

One way of minimising exposure is to take out appropriate insurance against cybercrime. To this end, Travelers has a series of technology products to cover risks including the growing threat businesses face from cyber criminals.

Two tailored products cover the technology industry: one for IT product and service providers and the communications sector; the other for manufacturers of electronic components and products. Travelers' Head of Product Development for Europe, Gerry Heffernan, confirms that both provide cover against a range of cyber-related exposures, including transmission of a computer virus to a third party and forensic investigation costs, in addition to data security breach notification costs and cover for business interruption.

"A significant exposure for many technology companies is business interruption or denial of service," says Heffernan. "A technology or communications service provider, for instance, runs the risk of losing its customer base if customers are unable to access the service as a result of a cyber attack."

Policyholders should have basic security measures in place, such as robust firewalls and anti-virus software that's regularly upgraded. However, companies shouldn't be lulled into thinking that just because they have anti-virus software, their networks are secure. Following an attack on the New York Times in 2013, software provider Symantec issued a statement that said, "Anti-virus software alone is not enough."

Symantec advised companies to adopt a combined approach to security. This involves controlling who is allowed access to sensitive information and when; encrypting data to protect it from theft; auditing network activity and alerting management to any incidents; and training staff in secure working.

The importance of this latter point was underlined by a survey of Irish businesses conducted by IT distributor Data Solutions in 2012. It found that 15% of business owners were worried about being attacked by hackers, with the vast majority afraid that security breaches would inadvertently be caused by their own employees. Two-thirds of the businesses surveyed stated they thought it was important that staff were educated about security, yet only one-third said that they currently run training courses.

It's a gap that needs to be addressed if companies stand a chance of combating the growing threat of sophisticated cyber criminals. ■

CASE STUDY

Global Aware International provides counter-terrorist/security and intelligent software solutions to customers around the world. The company can't afford to take risks with clients' information, says its Financial Director, Robin Rumsam.

"The data we hold is sensitive and so we take measures to protect it at every level, not just at the perimeter," says Rumsam. "For us the risk of a data breach and the resultant damage to our reputation means we leave nothing to chance.

"We see from the audit trails from our systems that our servers are regularly probed and so we take measures to ensure our servers and applications are patched to the latest levels. We have appropriate access controls to the data and we monitor closely our audit and log information to ensure we detect early any unusual behaviour and deal with it," explains Rumsam. "A data breach is very embarrassing but for a technology company, doubly so."

THIS ARTICLE FIRST APPEARED WITHIN TRAVELERS CODE RED, AUTUMN 2013 ISSUE.

Click here for more information on our Industry*Edge* products for the IT & Communications and Electronic sectors

INDUSTRY*Edge*®