THE NEW ERA OF DIGITAL FRAUD

By Nic FildesPublished September 1, 2015

With almost all business records now created and held on computers, the risk of digital fraud rises each year, but there are counter measures to hit back at the hackers

No matter how many moats, walls and booby traps companies set up around their critical digital information, the bad guys, as they are known in the cyber security industry, seem to get in.

Carphone Warehouse admitted in August 2015 that up to 2.4 million customer details had been accessed by hackers

Among the most recent victims was Carphone Warehouse which was forced to admit that hackers had gained access to as many as 2.4 million accounts with customer

details including names, addresses and bank information. Credit card information stored in an encrypted form could also have been accessed.

If there is a common denominator in every data breach, it is the claim by victims that the attack was “sophisticated”. All attacks, whether they are brute-force attempts to take down a web site or a dodgy USB stick that infects a corporate network, immediately become sophisticated once they succeed.

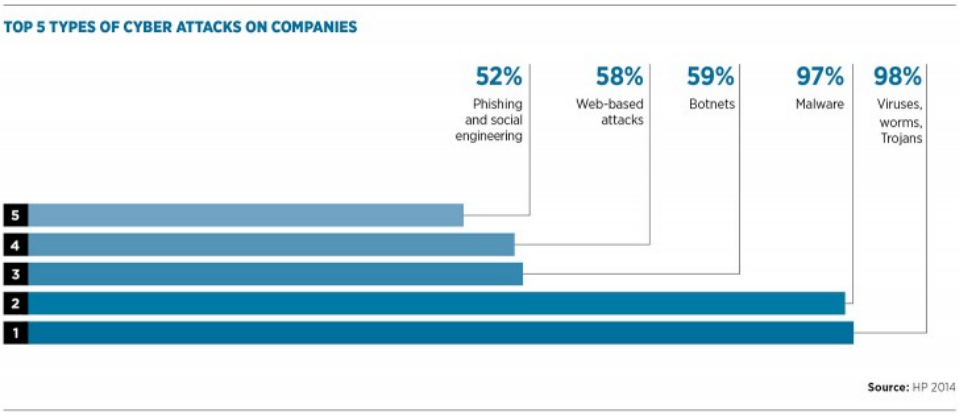
However, Dmitry Bagrov, UK managing director of technology consultants DataArt, doubts that many actually are. “Well they would say that wouldn’t they?” he says, misquoting Mandy Rice-Davies, on the so-called sophistication of an attack once a company realises its systems had been too vulnerable.

“With 90 per cent of all business records created and stored electronically, the risk of digital fraud is rising exponentially”

Basic tools

With 90 per cent of all business records created and stored electronically, the risk of digital fraud is rising exponentially. Yet what is alarming is how unsophisticated most attacks are. “It’s not like*Ocean’s Eleven* – these guys aren’t acrobats,” says Dave Palmer, chief technology officer at Darktrace. “Despite all the talk of armies of bad guys, the majority of people aren’t criminals and the majority of criminals are using basic tools off the shelf. We’re still in the era of low-hanging fruit where tricking people into watching a video or clicking on a link works.”

That threat has increased in the age of bring-your-own-device. Staff who take a tablet computer logged into the company network home with them run the risk of inadvertently opening the door to hackers. Mr Palmer notes repeated malware attacks on celebrity chef Jamie Oliver’s website. “How many people are thinking about cyber security when they look up a recipe for fajitas?” he asks.



Evolving threats

What is changing is the volume of attacks and what the bad guys are trying to do. James Lyne, global head of security research at Sophos, says: “We see in excess of 350,000 new pieces of malicious code every day, which means the chances of running into it are very high. What’s more, Sophos sees in excess of 30,000 infected web pages, which are typically small businesses that have been attacked and are now distributing malicious code to their customers. While it is easy to think of these attacks as the result of sexy high-tech hacking, the main attack vectors are still phishing e-mails and infected websites distributing malware.”

Customer bank details would usually be seen as the Holy Grail for hackers, but company data is now being used for industrial espionage and corporate blackmail. Even IT departments can be fooled into downloading patches that look legitimate but contain malware which can infect a whole organisation.

Darktrace’s Mr Palmer says many companies would have experienced internal extortion attempts but that blackmailers are now more likely to come from outside the company. Using ransomware, such as CryptoLocker, means outsiders can threaten to take down a company’s systems unless money is paid. Most companies are paying the fees, he reckons, as the cost of having a website go down quickly outweighs the ransom being demanded. “This is digitally enabled criminality,” he says.

Another fraud was revealed this month when a web of hackers were found to have made $100 million by breaking into the computers of business newswires and accessing corporate press releases before they were published. The scale of the fraud, perpetrated by hackers in the United States and Ukraine, shows how valuable non-traditional targets for data theft can be. Why bother selling a credit card number stolen from a company for $30 if you can get a run on a major piece of breaking news?

Luke Scanlon, technology lawyer at Pinsent Masons, comments: “This case highlights that too much of the focus of recent discussions has been on privacy rights. It shows that law-makers need to look more at the processes and controls to be put in place to help corporations protect confidential information. The involvement of cyber attacks and hacking in insider-dealing activities highlights a clear area of focus for market regulators along with other prosecuting agencies.”

Protecting interests

The irony is that for all the horrendous headlines suffered by the corporate victims of attacks, few have been hit as hard as would be expected. People are still buying Sony television sets and playing video games on PlayStation consoles. US shoppers still go to Target and shareholders still believe that people will continue to buy smartphones in Carphone Warehouse given its stock fell a tiny 1 per cent after it admitted it had been hacked.

Companies trying to deal with the relentless attacks – the equivalent of someone rattling the windows and doors of your house every minute of every day – probably feel they need to prepare for the worst. Small steps can, however, make a difference.

“To help thwart the cyber-criminal threat, everyone has to do their part and it’s surprisingly simple practices that make the difference – updating the software on your computer, in particular your web browser and popular software such as Adobe Flash, makes a huge difference,” says Mr Lyne of Sophos. “Running end-point security software and web-filtering software will also help keep your system clean. Finally everyone should be alert to scams. The old adage of ‘if it seems too good to be true, it probably is’ really does apply here.”

Darktrace believes that a more radical approach is needed. The starting point for any company needs to be that they have already been hacked and the best way to deal with it is to look for abnormal behaviour on a corporate network – a random laptop logging on or a worker acting irrationally at an unusual time, for example. Darktrace’s software, based on the same pattern-recognition techniques developed by software company Autonomy, acts like a burglar alarm that alerts the IT department to odd behaviour.

“We need an immune system like we have for the body. We can recognise the symptoms of polio and deal with it – we need the same for cyber security. In ten years, most cyber defence will be based on these principles. You can’t just look back and do what worked before. You need to be as flexible as a hacker,” Mr Palmer concludes.

Original article — http://raconteur.net/business/the-new-era-of-digital-fraud