PUTTING SECURITY ON THE BOARDROOM AGENDA

With the prospect of netting big money, criminals have moved away from scams on individuals and begun to focus on larger prey

Clad in a dark balaclava, the bank robber raises his pistol to a bespectacled teller, who deadpans: "You know, you can do this just as easily online." The scene is a 2006 cartoon from the *New Yorker*, and like much of the best humour, it carries a ring of truth. Criminals who stole a reported $80 million from the Bangladesh account at the Federal Reserve Bank in New York in March did so not by means of the gun and the getaway car, but by first installing malware on the bank's systems to spy on how it processed electronic transactions.

"Cyber criminals" are increasingly targeting financial institutions, having first cut their teeth on easier victims. "Criminals went after the retail sector first, such as Target and Home Depot in the US. Those guys have got better at security, so they're no longer becoming victims. Now, we're seeing incidents happen like the Bangladesh attack," says Mike Harris of Grant Thornton.

In a 2015 report on financial threats, the security software provider Symantec identified a noticeable shift in attack patterns, as criminals moved away from defrauding individual bank customers by using malicious software known as trojans. "It's almost easier to hit a bank and have a very big win rather than trying to hit multiple individuals. Financial trojans still exist but we saw a huge drop in the number of infections - a decline of 73 per cent compared to the previous year," says Orla Cox, director of security response at Symantec.

The report also found that trojan "families", though fewer in number, attacked more broadly in 2015, with 93 separate targets per sample. The most frequently targeted bank last year was located in the US and it was attacked by 78.2 per cent of the trojans which Symantec analysed. It said there were many more attempts at infection than actual successes, but warned that the new samples of trojans were very capable.

Joe Carthy, director of the UCD Centre for Cybersecurity and Cybercrime Investigation, says banks in turn are responding to the increasing rate of attack. "If you think of it from a risk perspective, if there is a serious cyber incident at a bank, the impact is potentially very large given the amount of money that could be lost. Up until now, we've seen low-impact attacks, whereas if criminals can get into the main banking network, it's like taking money out of the safe."

With the prospect of netting big money, cyber criminals are now prepared to play a long game, investing time to research and stake out victims before attempting a breach. Larger companies make the likeliest targets because attackers can easily find out about the company and identify key executives online. After the intelligence gathering stage, the next phase of the attack is often unsophisticated. The Bangladesh account attack is said to have started with a phishing email that tricked a bank worker into downloading malicious software onto the company network.

Business email compromise

Another email scam is known as CEO fraud, or business email compromise, which specifically targets an organisation's senior executives. Attackers craft a simple email and use techniques to make it appear to come from the chief executive, with an urgent request to a member of the finance department to transfer money to another account, supposedly to pay a supplier or agent. "The average loss is around $130,000 [€115,000], but in some cases, successful scams like this have seen more than $1 million transferred in one go," says Cox.

Security experts say shorter messages tend to be the most effective at fooling recipients. The emails may include wording like "I'm on the road, don't try to call me, I won't pick up", or it will make a reference to an upcoming deal involving the company – one which may actually be genuine that the attackers have learned about in preparation. As an added touch, the emails sometimes have the template "sent from my iPad" manually added – all designed to make the message appear as authentic as possible.

"It doesn't require malware or sophisticated techniques, it's just social engineering, and it's something the FBI have issued warnings about," says Cox. "It's tricky even for companies like us to block these emails, because they're simple and there's no malicious code. You have to be careful because you could block regular email. The simpler it is, the harder it is to block, ironically."

Third-party suppliers

Another route of attack is to target not the companies directly but third-party suppliers whose defences may be easier to breach than those of the intended victim. With so many multinationals based in Ireland, Harris says Irish companies in the supply chain to larger organisations will need to be aware of the risks. "If you look at some of the data breaches in the US, they came through third-parties. The Target breach, for example, came about through its air conditioning supplier."

Cox says Symantec has heard anecdotally of supply chain attacks. Multinationals are said to be responding to the risk by asking suppliers to provide security-specific certifications or to implement higher security controls such as encrypting email or financial transactions.

"These are extra controls that companies might not expect to implement, but I think it's going to become more commonplace," she says.

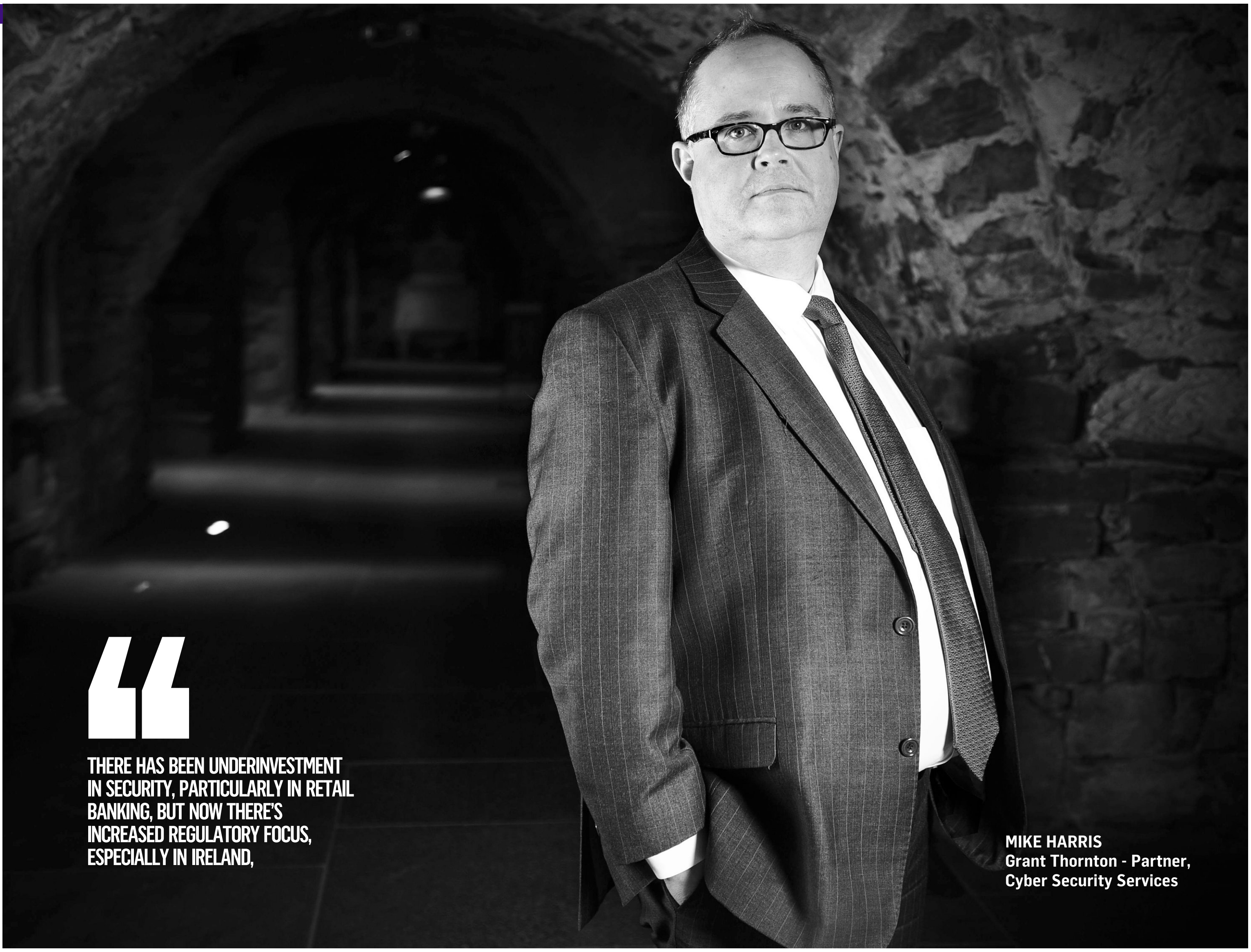
Harris expects increasing regulation

ORLA COX
Security response director at Symantec

> "It doesn't require malware or sophisticated techniques, it's just social engineering, and it's something the FBI have issued warnings about

JOE CARTHY
UCD Centre for Cybersecurity and Cybercrime Investigation director

> "If you think of it from a risk perspective, if there is a serious cyber incident at a bank, the impact is potentially very large given the amount of money that could be lost



"THERE HAS BEEN UNDERINVESTMENT IN SECURITY, PARTICULARLY IN RETAIL BANKING, BUT NOW THERE'S INCREASED REGULATORY FOCUS, ESPECIALLY IN IRELAND,

MIKE HARRIS
Grant Thornton - Partner,
Cyber Security Services

will lead to higher spending on cyber security in the financial services sector. "There has been underinvestment in security, particularly in retail banking, but now there's increased regulatory focus, especially in Ireland, and banks now need to spend more to remediate it," he says.

Cyber liability

Regulations are also putting company directors in the spotlight, compelling them to better understand cyber security as a business risk. Late last year, the law firm Mason Hayes & Curran launched an app which details various types of "cyber liability" and online risks, while drawing together the key areas for directors to consider. It also outlines both proactive and reactive strategies to manage cyber security.

Complicating the picture further, the financial services landscape is changing as challenger institutions like lenders and payment processors emerge with no ties to traditional banks. "These fintech companies are technology driven and they use the cloud. Banks have a lot of machinery around risk management. The challengers are more nimble from a technological perspective, but they may not know the regulations as well," Harris adds.

All of these trends are likely to mean cyber security will move higher up the agenda at boardroom level. "The fact that we're a small country on the western edge of Europe no longer means we're under the radar. We have a large indigenous funds industry that's being increasingly targeted. If you're one of the 200 or so people that sits on the boards of funds and asset management, do you know about this area and do you know your responsibilities?" says Harris.

Fortunately, Ireland has a model for how the industry can share information about common cyber security problems and discuss online threats. For the past decade, the Banking and Payments Federation's high-tech crime forum has been gathering senior executives from all of the major Irish banks, as well as An Garda Síochána and experts from UCD investigative centre for that very purpose. "I think our banks are as well prepared if not better prepared than other countries, but that's not to say they couldn't have a major incident," says Carthy.

SECURITY TIPS EXTRA STEPS TO PROTECTION

With cyber attacks increasingly using phishing emails and social engineering techniques, technological defences are just one part of ensuring a company is as well protected as it can be. Here are some other measures to keep attackers at bay:

■ **Use two-step verification**
Require a phone call in addition to email, when approving money transfers over a certain amount, to avoid being caught by a scam.

■ **Conduct regular user awareness training**
One of the most cost-effective measures is to teach staff to spot a fraudulent email and know tell-tale signs of a scam.

■ **Use specific anti-phishing services or email security tools**
These technologies help identify attackers' techniques such as "typosquatted" domains, which are intended to look like the victim company's actual email or web address.

■ **Carry out security audits**
Get an external consultancy to carry out spot checks on your in-house security, such as not leaving passwords written on post-it notes next to desks.