

Crime without borders

Fraudsters have been just as prepared as banks to make use of the advantages of operating online. A recent online discussion convened by *Operational Risk & Regulation* looked at how the threat is evolving and what banks can do in response

Operating online has tremendous advantages – demanding operations can be automated, information can be shared instantly around the world, and money can be moved without friction from account to account. Unfortunately, these advantages are not confined to the law-abiding world, and criminals are getting better at using them than banks.

“There are two main drivers of change,” Mark Büsser, president of the Swiss compliance & risk management software provider IMTF, says. “One is everything that is happening on the technology side, and the other is the development of the criminal or underground economy. The cost of labour in the underground economy is almost zero, and so the speed of evolution is much faster than it is on our side – that’s a major driver.”

Dean Goodlett, assistant vice-president and fraud investigations manager in the financial intelligence unit at Rabobank, adds: “It’s a global information age for the criminal element. Information is being shared back and forth around the world. Starter kits are available for sale online, so you have people who are not even committing crimes themselves but selling the ability for others to be able to carry out the crimes.”

The panel agreed that mobile phones, especially smartphones, were a new avenue of attack for criminals, as much as they were a new service channel for banks. And there are many problems with securing smartphones. Ben Knieff, director of product marketing at NICE Actimize, points out: “Most people are not protecting these phones, not even with something simple like a four-digit Pin number. Most people are just not thinking of them as computers.” Goodlett agreed: “We have to start to see smartphones as mini computers, subject to the same risks of intrusion.” But not everything that works for a computer will work for a mobile platform – for example, running constant antivirus software may not be an option because of the drain on the phone’s limited battery life.

In addition, the growth of online banking and customer service competition has not served security well, Knieff says. “Banks have been phenomenal at training their tellers and their sales staff to focus on customer service and cross-selling, but that has allowed great opportunity for attacks using social engineering – they get a call from a customer who has forgotten their password and think ‘OK, let’s get that fixed for you, here are a couple of questions’, but the answers to those questions could be on Facebook, for example.”

But there are reasons for optimism. Knieff continues: “We have done a good job of educating customers about spam and phishing attacks.

The panel

Mark Büsser, president, IMTF

Dean Goodlett, assistant vice-president and fraud investigations manager, financial intelligence unit, Rabobank

Ben Knieff, director of product marketing, NICE Actimize

Smartphones will need a shift in consumers’ views just as online banking did. And smartphones have new sensors, such as front-facing cameras and global positioning systems, which can be used to help the authentication process. There are opportunities as well as challenges.”

The panel also stressed that the security industry, like its opponents, should take every opportunity to share information, in particular the details of novel attacks. “What’s interesting is the shift in the industry from pushing the attacks off you on to someone else to taking the view that we should all co-operate in reducing the amount of fraud globally,” Knieff says. Büsser emphasises: “Sharing experience is very important. We have started to operate a scenario-clearing service.”

Key to any discussion of security is determining methods for measuring the success of a security strategy. This is not a simple task, Goodlett warns. “The problem with metrics is that we use them to quantify systems, but we don’t always qualify our metrics. For example, we had a cheque fraud training programme that reduced losses – so we were very happy – but the number of attacks had fallen as well in the same period, and to an even greater extent. So the reduction in losses was not necessarily proving anything. You need to qualify your metrics before taking them to senior management.”

The panel stressed another important, but often-neglected, point: the response to online fraud has to be immediate, stopping the fraud as it happens rather than simply logging and reporting it at the end of the day. Goodlett argues that “systems need to be able to make real-time decisions” and Büsser agrees: “Money is moving faster today. Everything has to happen faster, even in real time. Many systems are detection-based, but we have a real need for prevention. There is a lot of potential still on this side.”

To view and listen to the full proceedings of the *Operational Risk & Regulation* online banking and cybercrime webinar, visit www.risk.net/2116027