BERNARDO BÁTIZ-LAZO examines the history of attacks on ATMs to see what it can teach us about cybersecurity, and considers whether banks are facing a war that will never end.

Dispensing **wisdom**

Keeping cash and customer details secure has been a preoccupation of bankers for many years and it was no different when they adopted automated teller machines (ATMs). Bankers who underestimated the resourcefulness of criminals soon paid a price.

This was the case a couple of years after the first Swedish machines came into use. Withdrawals using fake cards started to happen when someone worked out the algorithm used to associate a card number with its PIN code. This was evident one Easter holiday when someone (or some people) travelled around Sweden, withdrawing money from each machine they visited. The theft only came to light when the holiday weekend was over.

Thieves quickly worked out that stealing from ATMs could be lucrative; they knew the machines were just sitting there, full of cash – that kind of temptation is hard to resist. Indeed, the motivation to steal will probably never disappear. So, when Dominic Hirsh, CEO of RBR London, invited me to the annual RBR Cybersecurity meeting in November 2017, I was intrigued to hear about the increasing risks and diversity of attacks faced by custodians of cash and digital money.

"The industry has seen a rise in the frequency of attacks as well as an increase in the variety of methods of attack. Some of the less sophisticated include the theft of the whole device."

ATMS UNDER ATTACK

The average cash machine in Britain is big enough to hold £120,000, although few are stocked with as much as this. The amount inside each can vary substantially, depending on a number of factors, such as the make and model of the device, whether it is installed on a bank's premises or not, the time of day, and which part of the country it is in. For example, during off-peak hours, most off-branch machines in the UK contain less than £10,000.

Not knowing how much is in a machine has not deterred the criminals; in fact, the

to contents

industry has seen a rise in the frequency of attacks as well as an increase in the variety of methods of attack. Some of the less sophisticated include the theft of the whole device, sometimes simply by ramming a car into the wall (a method known as "moon landing"). But more recently some gangs have refined their approach to melt or otherwise get through an ATM's protective layers to reach its innards. Once through, they can relay commands from a compromising device to the dispenser (e.g. "black box attacks") as well as using brute strength to force the machine to release cash.

Most often, however, criminals aim to capture customer details either at the card reader ("skimming") or elsewhere in the device ("deep skimming"). The industry has responded with different forms of protection, such as spoiling banknotes with special ink and using the kinetic energy of a moon landing against the criminals.

According to RBR London, at the end of 2016 there were 3.6 million ATMs in use across the globe. But, as the most common forms of attack suggest, it is clearly an impractical proposition to try to steal the whole of the stock of money within ATMs, as criminals would have to physically access each and every device in the world.

"Given the investments of banks, payment companies and FinTech start-ups in mobile payments, it is in their interest to press now for greater security and resilience."

ALL ELECTRONIC THEFT IS RISING

As more and more retail transactions are made through digital means, electronic theft – in all its various forms – is also on the rise. According to data from the Metropolitan Police, cited at the RBR Cybersecurity meeting, one in ten individuals has been subject to some form of cybercrime, such as payment fraud or a ransomware attack.

And it seems as if the criminals are turning their attentions away from individuals towards small and medium-sized enterprises (SMEs). Indeed, according to the same source, some 360,000 SMEs had suffered attacks, not all of them isolated, leading to losses estimated at just short of £2 billion in 2016.

LESSONS TO BE LEARNED

In this context, how can the future of cybersecurity be shaped by the lessons of the history of attacks on ATMs? These examples and anecdotes suggest custodians of money face a war that will never end, and which financial institutions will never win.

There is no room for complacency, of course, but it seems that being swiftly reactive is as important as being proactive. While the form, nature and sophistication of the attacks will evolve, this may not necessarily displace the criminals' tried-and-tested methods. It seems that there is an over-emphasis by banks on the security of individual customers, which appears to have left SMEs behind; more could be done by banks and other stakeholders to work together and in collaboration with SMEs.

Finally, it would be naive not to expect attacks to move to the mobile phone domain. Given the investments that banks, payment companies and FinTech start-ups have made in mobile payments, it is in their interest to press now for greater security and resilience. CB

Bernardo Bátiz-Lazo is a Professor in Business History at Bangor Business School.