PRESS RELEASE

London, 24th July 2017

ATM & Cyber Security 2017 – a collaborative approach to tackling cyber crime

Safeguarding ATMs has never been more of a challenge for deployers, with the ongoing threat of physical attacks and the increasing reality of cyber hacks. It is against this backdrop that RBR is organising its annual ATM & Cyber Security 2017 conference on 10th and 11th October in London.

Cyber attacks putting customer trust in jeopardy

For many years, banks and independent ATM deployers have been battling against physical ATM attacks. Despite advances in security technology, criminals remain one step ahead, meaning ATM deployers need to continuously refine their strategies and update their solutions. More recently, cyber attacks on ATMs have become a reality across Europe and further afield. RBR's Managing Director, Dominic Hirsch, explains: *"With cyber attacks, the threat is not just money that might be stolen or fines that might be imposed but most importantly the consumer trust, which, once lost, is extremely difficult to regain".*

International banks share pioneering initiatives for protecting ATMs

ATM & Cyber Security 2017 is the world's leading event on physical and logical ATM security. It provides a forum for banks and industry experts to discuss possible solutions to the many challenges they face. The event brings together 350+ senior bank executives, independent deployers, payment providers, law enforcement agencies, hardware and software suppliers and service providers to discuss the latest developments in the world of ATM security.

At the core of the two-day conference is a high-quality speaker programme covering a multitude of themes such as anti-cyber crime strategies, protecting against explosive attacks and ram raids, how to use biometrics, optimising CIT security and protecting client data. The agenda includes presentations from the Home Office (UK), Wells Fargo (USA), Visa (UK), Poste Italiane (Italy), Bradesco (Brazil), Barclays Africa (South Africa) and many more.

Cyber crime case study: The Cobalt Group's jackpotting spree

For ATM deployers across Europe and Asia, the threat of a logical attack became a reality in 2016. A gang of criminals dubbed the 'Cobalt Group' was reported as the most likely culprit behind this wave of hacks, which saw malicious software being deployed into ATM computers, manipulating the system to dispense cash. This type of crime is known as 'jackpotting' or 'cash spitting'.

The gang initiated infections via phishing scams, to gain access to the banks' networks. They were then able to make their way into individual ATM systems and plant malware. From then on, the group could send a remote command to any infected ATM, forcing it to spit out the entire contents of its safe. The 'jackpot' was collected directly from the ATM by a cash mule. It has been claimed that ATMs across Armenia, Belarus, Bulgaria, Estonia, Georgia, Kyrgyzstan, Moldova, the Netherlands, Poland, Romania, Russia, Spain, the UK and Malaysia were compromised.

How can deployers mitigate the risks?

To reduce the risks of such attacks, it is crucial that deployers adopt a mix of human and technical solutions. Staff training on topics such as password management and identifying suspicious emails is important, as are more technical solutions, such as encryption, whitelisting, firewalls, cloud security, DDoS protection and so on – ultimately every organisation will need a solution that is tailored to its specific requirements.

A case study "Hunting Cobalt" presenting further details on this attack will be presented at the ATM & Cyber Security 2017 conference in London on 11th October.

Latest security solutions unveiled at cutting-edge exhibition

Running parallel to the world-class speaker agenda is a dynamic exhibition where leading vendors* showcase their latest physical and logical security solutions. Extended breaks and a complimentary drinks reception provide ideal networking opportunities for generating new leads and re-connecting with industry peers.

To register your attendance, or find out how to get involved as a speaker, sponsor or exhibitor, visit www.rbrlondon.com/events/atmsec.

** Confirmed exhibitors include: 3SI Security Systems, Abloy UK, ATM Security Association, Axis Communications, Bastion, Cennox, Cyttek Group, Darktrace, dormakaba, GMV, KAL ATM Software, Lockpoint, March Networks, MIB Group, NCR, Oberthur Cash Protection, PINGuard, Sargent and Greenleaf, S21sec, Southco, Spinnaker and TMD Security*

Notes to editors

To discuss *ATM & Cyber Security 2017* in more detail, please email Emily Camara (emily.camara@rbrlondon.com) or call +44 20 8831 7318.

RBR is a strategic research and consulting firm with three decades of experience in banking and retail automation, cards and payments. It assists its clients by providing independent advice and intelligence through published reports, consulting, newsletters and events.