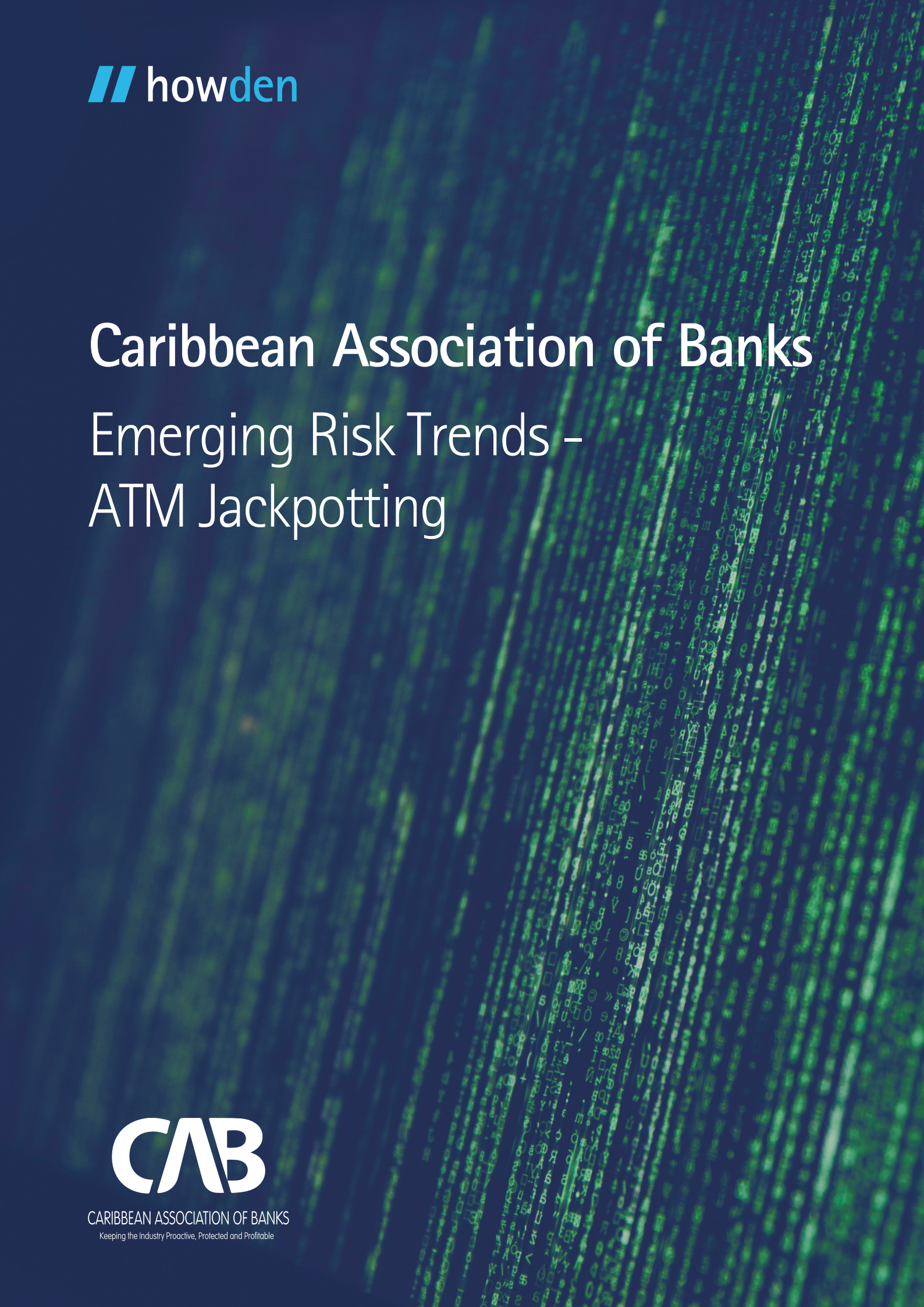
howden

Caribbean Association of Banks

Emerging Risk Trends – ATM Jackpotting



CAB

CARIBBEAN ASSOCIATION OF BANKS

Keeping the Industry Proactive, Protected and Profitable

Emerging Risk Trends
ATM Jackpotting

The first reported attack of ATM jackpotting was in 2013 in Mexico. The malware, called Ploutus, was identified as one of the most advanced ATM malware families in recent years.

One of the reasons the attacks took longer to spread to the Caribbean is because it may have been easier to get away with physically stealing ATMs and bribing individuals in Latin America than in the Caribbean.

This particular type of cyber-crime has been seen for years in Europe as well as in Asia. But it turns out one of the first instances of ATM jackpotting was not actually a crime. Hacker, Barnaby Jack demonstrated how ATM vulnerabilities could be exploited in an effort to raise awareness about jackpotting.

What is Jackpotting?

The heists, which involve hacking ATMs to rapidly shoot out torrents of cash is also known as 'logical attacks'. This simply means that cyber thieves - often dressed as technicians to deflect suspicion - physically install malware onto ATMs giving them control over how much money gets dispensed at any given time. Once the machine is taken over, they can be forced to dispense money at a rate of 40 notes every 23 seconds until empty.

The malware installers have been clever, using endoscopes (narrow, tube-like medical devices with cameras on the ends typically used to see inside the human body) to look inside each ATM. Once they find a place to attach a computer cable, they synchronise their laptops to the machine's computer.

How to protect against Jackpotting attacks?

Experts advise ATM operators to upgrade their operating system, use robust physical ATM locks and add two-factor authentication to ATM access controls. Some ATM operators using the new Windows 7 have been successfully attacked within the last 3 months. There is not one magic solution to solve the problem.

For every single of one these attacks, the perpetrators need good physical access and need a portion of time where they can either pick the lock or use some type of key they may have obtained from someone. You can have the latest and most advanced software but with physical access they figure out ways to remove the protections. This is not a software problem, it's a hardware problem.

An immediate preventative measure is to increase physical security around existing ATMs as one of the simplest and fastest solutions to the ongoing jackpotting attacks. Stand-alone ATMs in pharmacies, retailers and drive through ATM's have been the most common targets so far.

How does insurance help?

Our clients have the benefit of their own, bespoke Crime and Cyber Crime policy, which ordinarily covers losses arising out of ATM Jackpotting but not all policies do. For example, certain policies usually only protect policyholders against losses and expenses caused by the physical theft of the ATM or fraud carried out by an employee or third party. Policyholders should always refer to the applicable terms and conditions to see what cover they have and whether they qualify in any given situation.

Howden has a modular approach to Crime and Cyber insurance, which allows clients to tailor their cover to match their risks. If you would like to discuss your current level of cover and whether a specific cyber policy is necessary, we would be happy to discuss your requirements in further detail.

For any questions or additional information, please contact:

Mary Popo
mary.popo@cab-inc.com
Blair Buchanan
blair.buchanan@howdengroup.com