Executive Summary

Securing automated teller machines (ATMs) has been keeping bank security officers up at night ever since the first one was introduced in the 1960s. ATMs have always been subject to physical theft, of the machine itself or the cash inside. Today, however, the fastest-growing risk to ATMs comes from cyberspace. Not only do malware and hacking threaten the individual machine that is under attack but they also put the entire network at risk. As banks adopt new policies and procedures for keeping ATMs secure, they must also ensure they are meeting all appropriate regulatory requirements. At the same time, financial institutions must minimize the impact of these measures on the total cost of ownership (TCO) of their ATM network.

ATMs At Risk Around The World

ATMs have changed the face of consumer banking. What was once a competitive advantage—24x7 self-service banking—is now a business imperative resulting in more than 3 million ATMs in service around the world.1

The challenge for banks is keeping these broadly dispersed machines secure. Decades ago, Willie Sutton reportedly replied, when asked why he robbed banks: "Because that’s where the money is." ATMs operating throughout cities, towns, and rural outposts around the world hold cash ready for dispensing. Guarding a network of hundreds of these stand-alone machines is an enormous challenge for modern financial institutions.

Physical attacks have always been a concern. From the advent of the ATM, thieves have used tools such as torches, forklifts, and even earthmovers to physically remove ATMs from their moorings. Their intention in these types of attacks is to access the stolen cash once the machine is somewhere less public. Thefts of this type continue, as do physical attacks on individuals after withdrawals. In Latin America, 31% of people report that they do not feel safe using an ATM.2

Certainly, bank security officers need to continuously monitor and respond to these concerns. But they also need to protect their systems against the latest threats, which generally come from the 21st-century attack vectors of fraud and cyber crime.

Fraud Threats Continue

Criminals perpetrate ATM fraud by impersonating users to make withdrawals. They might steal bank card data through “skimming,” in which a device physically inserted into the ATM copies card data when a user initiates a legitimate transaction. They might confiscate debit cards through “card trapping,” in which a tool inserted by the thief prevents the ATM from returning a user’s card, trapping it in the machine for the thief to retrieve.3 They might also hide a video camera near the ATM to capture users’ PIN information.

Thieves who “skim” card data generally create a dummy card with a magnetic stripe identical to that on the victim’s card. They use the fake card to make withdrawals from the victim’s bank account until the fraud is discovered.

Defenses against skimming and counterfeit cards include various physical measures, from a PIN shield screen and PCI-certified keypads to biometric authentication. For example, starting in 2006, banks in Japan have installed 80,000 biometric ATMs that identify users based on fingerprint recognition, or even the pattern of capillaries in the finger or hand.4 ATMs of the future will likely incorporate iris scans as well.
ATM Cyber Threat Is Growing Rapidly

As troubling as physical attacks and card fraud may be, the fastest-growing threat involving ATMs comes from hacking and malware. The National Bank of Blacksburg, a small institution in Blacksburg, Virginia, lost a total of $2.4 million in two attacks that occurred in May 2016 and January 2017. The criminals executed a phishing scheme on a bank employee. They used the information the scheme uncovered to compromise the systems with which the bank manages credits to and debits from customer accounts. Once in those systems, they removed the bank’s preset limitations on withdrawals. Then, the thieves began a massive ATM cash-out scheme, making large withdrawals, presumably using cards that they stole or replicas of legitimate cards’ magnetic stripes.

The Cobalt attack in Thailand in 2016 was even more disastrous. Malware installed on the bank’s internal network enabled criminals to remotely, and simultaneously, access a large number of ATMs. The bank lost nearly US$3 million in the attack. Exacerbating the problem was the fact that it took two weeks to discover—during which nearly half the bank’s ATMs were out of commission.

Perhaps the boldest attack, with the broadest reach, was perpetrated on India’s Cosmos Bank in August 2018. The scheme started with a malware attack in which hackers (believed to be in Canada) stole account information on holders of the bank’s Visa and RuPay cards. It concluded with a cash-out scheme similar to the National Bank of Blacksburg attack. Approximately Rs 94.42 crore (US$12.7 million) was stolen via around 12,000 ATM transactions across 28 countries during a period of two days.

Appropriate Security Is Imperative

For security experts, the lesson learned from these and other well-publicized cyberattacks is that ATMs must be included in a bank’s branch and corporate network security strategy. It is a lesson applicable to institutions of all sizes. The average loss in an ATM attack is US$50,000, but obviously the damage can be much greater. Considering the pervasiveness of the threat, even the average loss is a penalty that banks cannot afford to ignore.

Security technology plays a key role in threat mitigation. If the network is poorly designed and the security infrastructure is unsegmented, threats can spread more rapidly from machine to machine. This puts at risk every server and desktop computer in the bank’s headquarters and branch locations. It also exposes ATMs to more threats than they would face in a security infrastructure that prioritizes information sharing among devices, visibility across the bank’s attack surface, and isolation of detected attacks.
**Business Challenges**

On top of technical considerations, securing a network of widely dispersed ATMs creates a number of business challenges for banks. Key among these is compliance. Financial institutions must comply with government regulations in every jurisdiction in which they do business. This means banks with ATMs in multiple countries will have to meet an assortment of IT security standards across their ATM network.

Financial institutions also need to consider how their practices meet the cross-border regulatory framework of the Payment Card Industry Data Security Standard (PCI DSS). The PCI Security Standards Council is a global forum, founded by leading credit card providers, that publishes security standards designed to protect cardholder funds and data. PCI compliance for ATMs is an important part of a financial institution’s overall compliance strategy. Banks scrutinizing ATM security may find that meeting the PCI DSS requires operating system upgrades on the machines. They also may need to develop a more comprehensive and integrated approach to IT security overall. In addition, PCI DSS compliance requires effective and transparent processes for installing security patches, to ensure that individual ATMs are always up to date.12

Another set of standards with a broad reach is the Good Practice Guide (GPG) from the U.K. government’s Communications-Electronics Security Group (CESG). GPG 13 details 12 proactive monitoring controls intended to increase awareness of network vulnerabilities, help deter incoming threats, and support detection of and defense against attacks.13 These controls are suggestions, not requirements, for most organizations worldwide, but they are widely considered to represent IT security best practices.

The European Union’s General Data Protection Regulation (GDPR) also lays out very clear standards for data security. Any company that does business in the EU or collects or stores personal information on EU citizens must comply with GDPR.14 Because ATMs obtain user names, account information, and PINs, a bank’s IT infrastructure must be GDPR-compliant if EU citizens use its ATMs. Compliance requires these institutions to deploy state-of-the-art systems for securing personal data, including use of encryption technologies.15

**Cost Of Ownership and Staffing Concerns**

As they work to comply with the various security regulations, banks with dispersed ATMs must carefully consider costs and staff resources. Effective and compliant security practices may require frequent patching on the machines. If the bank’s security infrastructure does not enable centralized management, staff may have to travel to each ATM every time the machines need a security update. This dramatically increases the TCO of the network of ATMs.

Each new machine that adds travel time to typical system maintenance activities increases the staff time required to secure the bank’s ATMs. If the institution is able to expand its security staff to manage the machines, doing so increases staffing costs. However, adding personnel may not even be an option for some banks today.

Companies around the world face a shortage of experienced and knowledgeable IT security staff. In some regions, the situation is acute: Security teams are perpetually understaffed and have difficulty filling open positions. Any organization facing this type of resource constraint needs to ensure that the experts it does have on staff are focused on strategic tasks. Rote activities such as driving from ATM to ATM to apply security patches not only increase staffing costs but also divert the security team’s attention away from more value-added activities.
Inefficiency Weaken Security

IT security teams struggling to manage updates across many dispersed ATMs may be tempted to ask local employees to apply security patches instead. However, staff who are not security specialists may make mistakes that reduce the effectiveness of the security update and perhaps expose the ATM to vulnerabilities.

A related risk is that manual processes for patching and updates may lead a financial institution to dedicate insufficient resources to ATM security. ATMs often do not fit within the scope of the corporate patch management systems that banks use for servers, desktop computers, and networking equipment. Thus, the institutions may need separate policies and procedures for keeping ATMs up to date. If applying a security patch requires travel to dozens, hundreds, or even thousands of machines, an already-overstretched IT team may be stretched even further. Staff may not reach every ATM with every patch in a timely manner. It is even possible that some far-flung machines may not get updated at all, as security staff juggle myriad competing priorities. Even when security teams can keep all their ATMs updated, manually managing dispersed machines may reduce the effectiveness of network security overall. If monitoring threats requires staff to collect data from individual machines’ log files, the security team may not recognize zero-day threats right away.

Further, if security solutions are not integrated throughout the corporate network, the bank’s security products will not respond to threats in a unified manner. Security solutions guarding executive desktops or the corporate data center may not be alerted immediately when an ATM’s security solution detects an attack. Such a lack of visibility into threats and lack of coordinated response networkwide undermine a financial institution’s overall security posture.
Conclusion

Banks looking to secure a network of hundreds to thousands of ATMs have their work cut out for them. Every machine represents a potential point of vulnerability for the customer cards it processes, for the cash it stores, and for the corporate network as a whole. Securing ATM funds and users’ personal data, while complying with all applicable regulations, is a challenge in the best of times. When staff resources are tight, applying appropriate ATM security becomes almost impossible if the financial institution does not have tightly integrated security across its attack surface.

ATMs are where the money is, so they will always be attractive to criminals. However, a sophisticated and integrated security architecture, with central monitoring and control, positions banks to detect and defuse the unforeseeable threats of the future.

5 Ibid.
9 “India’s Cosmos bank suffers global ATM cash-out attack,” EAST, August 14, 2018.
10 Ibid.
14 “General Data Protection Regulation (GDPR),” Intersoft Consulting.