

ATM CRIME: AN EVER-EVOLVING GLOBAL THREAT

Meet both current and potential security challenges with a multi-layered approach is the advice to Australia's bankers from one of the ATM industry's leading global players.



Vice president and managing director, Diebold Australia

The vulnerability is around magnetic stripes, and while the stripe has some value, as does the PIN, the real prize is the combination of customer information.

JAMES PETIT

ATM SECURITY IS an industry issue and requires an industry response, says James Petit, Diebold's vice president and managing director for Australia and New Zealand.

"The vulnerability is around magnetic stripes, and while the stripe has some value, as does the PIN, the real prize is the combination of customer information.

Petit warns that for organised criminal gangs, there's a compelling ROI argument from their point of view to move operations into Australia.

"They're quick, they're nimble, and they've got an R&D budget," he says.

"This is where an industry leader in security like Diebold can bring in a multi-layered approach, around the device, around the software, around the surveillance, around the monitoring.

"What we're also advocating is more collaboration between financial institutions, law enforcement, and technology providers."



There are already models in other jurisdictions where collaboration is proving effective

CHUCK SOMERS

Vice president, ATM security and systems for Diebold, Inc.

COLLABORATION ACROSS THE financial services industry is proving useful in countering the collaboration between criminal gangs, according to US-based Chuck Somers, vice president, ATM security and systems for Diebold, Inc.

"We have identified websites that offer card and PIN info on a wholesale scale," he says.

"This is an organised crime skimming operation, where there is disaggregation of the criminals' supply chain into separate 'centres of excellence', from the manufacture and sale of cards and machines, to theft via those cards. It is a major problem for law enforcement.

"It's the mules who get arrested, never the brains behind the operations."

There are already models in other jurisdictions where collaboration is proving effective, Somers points out.

"For instance, EAST (European ATM Security Team) is an example of what's being done elsewhere to combine information from all the institutions and geographies in the SEPA (Single European Payments Area) to identify industry trends, without naming individual banks," Somers says.

"Because it's being done by a third party – and an industry organisation – it's more likely that information will be shared."

From the day automated teller machines (ATMs) first appeared, financial institutions have made it a priority to secure them.

In the more than 40 years since the ATM was introduced, criminals have become increasingly sophisticated. They strive to breach the machines, trying to get to either the cash inside or the account information of the consumers who rely on the devices for their banking needs.

Today, criminals perpetrate ATM crime in a variety of ways. Physical assaults, such as ramming terminals or attempting to remove them from their locations, are the most brazen. Less violent, but more threatening, is the installation of malware to infiltrate the ATM's internal data network and enable the theft of account information.

Skimming and trapping methods steal magnetic stripe data and PINs while unknowing customers complete transactions.

In Europe, the European ATM Security Team (EAST) reported that ATM-related fraud losses totalled €312 million for 2009. Between 2008 and 2009, ATM attacks rose 8 percent, from 12,278 fraud incidents to 13,269, in the 32 countries that are a part of the organization.

Clearly, ATMs remain very much under threat globally.

To anticipate and mitigate ever-evolving threats to the self-service channel, financial institutions must be vigilant in their efforts to protect ATMs from a variety of attacks, from the most basic physical violations to the most sophisticated network schemes.

Understand the security landscape

Even as new innovations in ATM security are developed, the threat continues to evolve. The most current information and tools to help criminals breach ATMs are readily available via the internet.

Thieves are increasingly organised and able to commit crimes rapidly around the world. It's becoming more difficult to apprehend them.

Some skimming devices, for example, are so advanced that they employ Bluetooth technology to enable the wireless transmission of stolen card data and PIN information. The use of such technology means thieves no longer need to return to the ATM to retrieve the skimming device and stolen information, thus decreasing their risk of detection.

At the same time, financial institutions, in growing numbers, are changing the service model within their branches, driving basic transactions – such as withdrawals and deposits – out of the teller line and assigning them to the ATM.

With the ATM channel becoming even more pervasive, the assets and brand reputations of the world's financial institutions are more dependent than ever on effective ATM security solutions.

Take a multi-layered approach

Creating and executing an effective strategy for ATM security is among the biggest challenges facing financial institutions today. Meeting the challenge requires the implementation of a comprehensive, multi-layered approach to security that includes hardware, software and services. Financial institutions can gain valuable assistance by forming a strategic alliance with a proven security provider.

A third-party expert can help develop a strategy that proactively looks at the self-service experience from a broad security perspective. This comprehensive view encompasses physical and logical security, as well as fraud detection. The multi-layered approach includes assessing risk for each terminal based on location and environment while also educating consumers about good security practices.

Fight back against skimming

The multi-layered approach of combating ATM crime extends to specific defences against skimming, considered by financial institutions around the world to be today's greatest threat to ATM security. First identified in Europe, skimming is a crime of low risk and high reward, typically requiring only the attachment and later detachment of skimming devices to ATMs in order to obtain consumer card data and PINs.

It is a threat not just to ATMs, but to all self-service technology, from point-of-sale devices to self-service fuel pumps in petrol stations to check-in kiosks at airports.

Financial institutions must implement anti-skimming solutions that offer multiple layers of protection. The protection should range from basic solutions for card-reader security to higher levels of fraud mitigation, such as skimming detection alerts and real-time ATM security monitoring.

Create a customized solution

Financial institutions can help mitigate ATM crime by investing in a strategic alliance with an expert that can develop security solutions customised to their needs. Believing security is at the core of any ATM network, Diebold is a proven resource in developing industry-leading solutions to physically protect the ATM, safeguard the data assets of the ATM and its users, and secure the entire ATM environment.

Diebold combines its roots in security with financial self-service expertise, to ensure it understands the very latest security risks facing financial institutions, and can deliver maximum protection for their assets and customers. The global ATM Security team at Diebold is helping to fight evolving threats to ATM integrity by delivering customized, seamlessly integrated, multi-layered security solutions.

For more information, including a white paper offering a closer look at a multi-layered approach to ATM security, please visit: www.diebold.com/atmsecurity.com

