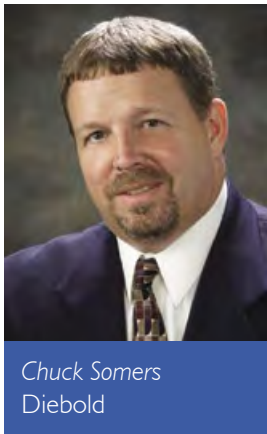


DIEBOLD PERSPECTIVE

No boundaries: ATM crime increasing globally

Combat ATM threats through professionally designed multi-layered security



Chuck Somers
Diebold

By Chuck Somers, Vice President, ATM security and professional services, Diebold

It's a growing global problem: criminals on every continent are becoming smarter in their efforts to commit fraud and sophisticated crimes against financial institutions and their customers. Thieves are releasing malware that infiltrate financial institutions' networks to steal sensitive information. They are attaching unauthorised devices to automated teller machines (ATMs) to seize customer transaction data and wipe out bank accounts. It's no wonder identity theft was cited as one of the top three life concerns of consumers across every age group in a study commissioned by Diebold in 2008.

What's worse is that thieves aren't just getting smarter – they are organising their ranks, which makes combating attacks increasingly complicated. Today, a crime committed in one country can be perpetrated the next day halfway around the world. In Europe alone, the European Network and Information Security Agency reported that total losses from ATM crime in 2008 reached €465 million, which is up 149% from the previous year. 10,302 of those attacks involved skimming.



In the past, the financial services industry has been relatively reactive in combating ATM crime. But there is a growing awareness that the industry must become more proactive in the battle against this threat, and that if joining forces works for criminals, then it can be advantageous for financial institutions, law enforcement and vendors as well.

Accountability across the ATM channel

ATM security is a responsibility shared by every entity in the retail delivery channel – consumers, financial institutions, vendors and security providers. For consumers, awareness and simple practices such as keeping PINs private, visiting well-lit ATM locations and shielding the number pad are ways to help keep safe. For financial institutions, forming a strategic alliance with a proven security provider can help dramatically in deterring crime and protecting assets and brand reputation against high-profile attacks. ATM security is one of the most technically challenging areas of a financial institution's operations and one that requires critical attention. The Financial Services Authority mandates that all UK financial services companies implement policies and procedures to protect consumer data and mitigate the risk of fraud.



Software or hardware alone can't do the job. Without a multi-layered approach to protection, financial institutions can spend exorbitant amounts of capital and get disappointing – and damaging – results. By partnering with a security professional such as Diebold, with a dedicated, global team of resources, financial institutions gain access to comprehensive security solutions tailored to their specific challenges.

Close the doors on malware

Cyber thieves will stop at nothing to gain access to sensitive data. Financial institutions must take steps to implement the industry's most effective security technologies and lock down their ATM fleets at every point of vulnerability. Strong firewall and intrusion detection is critical for monitoring and controlling traffic in and out of the network. Some of the most essential technologies include:

- Strong firewall and blocking capabilities for protecting against malware before it can enter the ATM system
- Threat scanning that tracks behaviours of unknown applications to enhance detection and reduce false positives
- Threat landscape intelligence that results in actionable protection and peace of mind against evolving attacks.

Financial institutions must implement security technologies that work at the firewall and beyond, which constantly monitor, analyse and authenticate

all sources attempting to connect to the ATM. An effective solution should also offer best-in-class malware protection, including USB blocking that limits access to all but the required ports on the ATM. Furthermore, antivirus and antispyware protection with automatic updates are required to ensure effective ATM security.

In a climate of increasingly aggressive cyber threats, enlisting a security services provider to implement and manage a comprehensive security programme helps financial institutions proactively manage these threats. Only by investing in proactive measures with proven security experts can the industry effectively strike back at cyber criminals. In today's world, the cost to financial institutions of taking no action to protect sensitive customer data or their own assets is immeasurable.

Diebold views security as the mainstay of the ATM network. We have placed security at the core of our business for more than 150 years. Diebold's team is committed to providing a multi-layered approach, encompassing physical, logical and fraud detection technologies in a fully integrated system to help protect consumers' assets as well as the reputations of financial institutions. ■

For a free ATM Security position paper and more information about how you can help protect your customers and company against emerging threats, visit www.diebold.com/protect.

There is a growing awareness that the industry must become more proactive in the battle against ATM crime

