DIEBOLD NIXDORF PERSPECTIVE

ATM security management: know your options

By David Raj, Head of Rapid Response Team, Information Security, Diebold Nixdorf

As risks have evolved in the self-service channel, managing its security has become more complex and more important. Beyond the emergence of new threat vectors, there are more interconnected channels to lock down, as well as varying defensive considerations required across generations of ATMs from multiple manufacturers. There is constant pressure to avoid monetary and reputation loss and to comply with changing regulatory requirements and industry standards in the process. While there is no one-size-fits-all solution, there are options available to financial institutions (FIs) so they can protect their ATMs and network and ensure consumer trust while providing secure services.

A successful attack on an ATM can lead to monetary losses, but that is far from all: it can lead to a loss of trust in the bank and long-term damage to its reputation. In a recent survey, 57% of consumers claimed they would stop spending with a business for several months after a security breach has occurred, and another 41% said they would *never* return to a business after it has been compromised[1]. Those are pretty compelling reasons to take every possible step to prevent attacks from succeeding.

It's easier said than done. Breaches have grown in regularity and sophistication over the last few years and every channel is under attack. In Europe, the number of cyber/logical attacks on ATMs grew by 44% from 2019 to 2020, and losses due to explosive attacks rose 39%. At the same time, the number of data attacks – especially skimming – has gone down. Unfortunately, this type of attack still makes up a large portion of the losses incurred: in Europe, €218 million were lost due to data fraud in 2020, and banks are often only able to recover less than a quarter of what was stolen[2].

[1] PCI Pal, June 2020

[2] *European Payment Terminal Crime Report Full Year 2020,* EAST, 2021 / *Global Banking Fraud Survey,* KPMG, 2019

So, what can be done? Let's take a quick look at the types of attacks FIs must protect themselves against:

- ***Data attacks*** attempt to gain physical and/or digital access to card data. Skimming technology in particular has been getting more advanced – some skimmers are now as thin as paper.
- ***Physical attacks*** are aimed at gaining physical access to the ATM's cash, and most consist of explosives or ram raids that destroy the ATM. They can be extremely costly and life threatening for bystanders.
- ***Cyber attacks*** aim to gain physical and/or digital access to systems and communications data and/or the ATM's cash. Jackpotting attacks have grown the most out of all attack scenarios.

As a defence contrivance, FIs should take a holistic approach, securing every transaction and connection. They can achieve this by minding three key principles:

1. ***Innovation***: As the threat landscape is constantly evolving, it is essential to make use of technologies that address new security threats against ATMs, payment devices and networks.
2. ***Integration***: We recommend integrating a layered security approach as the most effective means to establish trust and deter security threats. This practice spans across more than just the ATM; it also includes other channels and networks.
3. ***Information***: Proactively tracking regulatory initiatives and global security trends by collaborating with security agencies can help FIs protect themselves against potential threats and, when vulnerabilities are recognised, take corrective action quickly and effectively.

When dealing with security, experience can make the difference. For more than 160 years, Diebold Nixdorf has protected people, data and assets around the world. The DN Series™ features intelligence driven, targeted security solutions that mitigate risks and balance your business needs with your consumers' expectations for privacy. ■

To learn more, visit us at DieboldNixdorf.com/Security

David Raj
Diebold Nixdorf

Breaches have grown in regularity and sophistication over the last few years and every channel is under attack

Diebold Nixdorf