Diebold Nixdorf

Under Attack from all sides? Protected from all sides!

By Norbert Knievel, Head of Banking Thought Leadership, Diebold Nixdorf

Wherever cash, customer and financial data play a role, security must as well. These assets are some of the favored targets for attackers of all stripes—brutal physical, sneaky data, or sophisticated cyber attackers—which is why security continues to be a hot topic at the ATM. As a key pillar of financial institutions' (FIs) service strategy, providing users with a secure transaction is not only critical to customer satisfaction but even a prerequisite.

WHAT ARE THE KEY CHALLENGES?

- **Compliance:** The constant flow of new compliance requirements from global, regional, and national standards like PCI-DSS, card schemes, and others is hard to keep up with, and if you fail an audit, you will likely be sanctioned. This may still be better than the alternative: intentional or accidental fraud resulting in financial and image losses.
- **New Attack Vectors:** Staying secure long term is difficult due to new threats being developed or the migration of attacks into new regions. Especially zero-day threats in cyberattacks are difficult to protect against—79% of financial CISOs in one survey said threat actors were deploying more sophisticated cyberattacks[1].
- **Increased Attacker Organization:** While tools like the darknet have been used by attackers for years, for example, to purchase skimming devices, what we are witnessing in some regions is a new level of organization among ATM attackers. Take the strain of explosive attacks in Germany: In 2022 there were almost 500 attacks—more than 1 per day. Law enforcement agencies suspect the cash attackers earn is funneled into further illegal activities like drug trafficking.
- **Risks in the Chain:** The number of people and factors involved in an ATM fleet varies, but each can become a weakness in the chain and must be monitored and secured, including, but not limited to, consumers, branch staff, and cash transport operatives. Forms of attack like social engineering that manipulate people into giving attackers access based on false claims are common: nearly 80% of FIs said attackers were leveraging such highly targeted attacks[2].

WHAT STEPS CAN YOU TAKE TO SECURE YOUR SELF-SERVICE CHANNEL?

As a global partner for self-service hardware, software and service solutions with security experts around the world, Diebold Nixdorf has the unique, all-round capabilities and experience needed to provide threat intelligence regarding trends in different areas of the world. Our specialists have identified 7 steps, or metaphorically speaking, shields to secure a self-service fleet long-term. Here they are:

[1]https://purplesec.us/resources/cyber-security-statistics/#Financial
[2]https://purplesec.us/resources/cyber-security-statistics/#Financial

The 7 Shields to Protect the Self-Service Channel

Security Assessments ensure your self-service channel continues to be secure and can expose weak points before they are exploited. This is critical as attack patterns and security technology develop quickly.

Physical Security protects against attacks that use brute force to get to the cash inside the ATM but also against any attempt to get into the chassis to install fraudulent devices in or on the ATM. Measures range from enforced steel plates to sensors.

Data Security focusses more on protecting user data both by improving the privacy of the transaction with low-tech steps like visual barriers and mirrors and using high-tech device recognition and jamming technology.

Cyber Security is growing more relevant as cyberattacks have become more common with the spread of IoT-driven connectivity. Securing the communication between components of the ATM and the host, as well as preventing unauthorized access to devices and information, are effective countermeasures.

Security Monitoring can ensure a quick reaction to an attack, which can make a decisive difference. Using modern tracking and analysis programs you can closely monitor your self-service fleet to detect possible fraudulent activity in real time.

Process, Procedures & Compliance are necessary to avoid internal and external fraud—both caused by negligence or malicious intent. Secure and compliant procedures should be implemented throughout an ATM's lifecycle: The development process, the installation, and the day-to-day operation.

Cooperation & Collaboration like information sharing among all players—financial institutions, law enforcement, and ATM manufacturers, software, and service providers—is key to quickly analyze and counteract new security threats. A necessary step to counteract organized crime groups on the side of attackers.

WHAT ARE THE BENEFITS OF A MORE SECURE ATM FLEET?

Improved Brand Image

Any publicity is good publicity may be correct in many cases, but you do not want to be in the news due to a security breach or successful attack. Even one case may damage your brand for years—especially since people tend to remember bad experiences better and longer than good ones. In this case, remaining out of the spotlight is the way to go.

Trust as a financial services provider

Fintechs keep encroaching on the business of banks and other more traditional FIs. One key asset the latter still holds over the newer competition is the trust that consumers associate with them. However, this trust has been shaken, and you should do everything in your power to limit further stress on the relationship.

Attractiveness as an employer

The war for talent has also reached the financial sector, and there are many struggling to fill positions across their organizations. Consider two banks that are both looking for tellers, where would you rather work: At the one that is being targeted by attackers exploiting a weak point in their armor, or the one that has not been attacked because attackers determine the risk to be too high?

Reduction of financial losses

Lastly, both failed audits and successful attacks are costly. With the more brutal physical attacks, damage to devices and surrounding structures can quickly reach more than $1million, but even less destructive attacks like skimming cost $100,000 or more. And that is without considering the financial effect of lost business from loss of trust and increased insurance premiums.