How to manage payment security as effectively as enterprise retailers

By Wayne Steppe

26 Apr 2024

While the majority of people may not think twice about how they pay for their goods, ever-evolving retail payments, both in person and virtually, keep many CIOs awake at night worrying about where the next attack will come from and how best to mitigate against it.

Image supplied

Retailers have no choice but to keep pace with rapidly evolving tender types that bring with them massive cost and complexity considerations and most importantly, added security and compliance risk.

While this is certainly true for tier one or enterprise retailers, mid-market retailers often don't have entire departments dedicated to security and compliance adding to the pressure, because while they may not be as big with as many resources as the enterprise retailers, they are often competing for the same consumers meaning they can't be left in the dust.

Retailers must cater for all payment methods

Some consumers still prefer to pay with cash while many others enjoy inserting or tapping their debit or credit cards. Some savvy consumers opt to tap their smartphones with the likes of Apple Pay or Google Pay, while others still prefer scanning a QR code or using the fairly new interbank instant payment app PayShap. Retailers need to cater for these ever-evolving tender types, including vouchers, mobile wallets and cryptocurrency.

Ever-increasing payment options, which brings increased attack surfaces, shines the spotlight on security. A security breach comes with an obvious financial risk, but there are also reputational, compliance and legal risks to consider.

Smaller companies often cannot take on the financial burden of having to invest in an array of different security and compliance obligations. This opens them up to vulnerabilities which they simply cannot control.

A partner, who brings enterprise experience and solutions to the mid-market segment, effectively levels the playing field because a one-stop solution that's encrypted end to end enables smaller retailers to serve customers as effectively and safely as their tier one counterparts.

Security standards

With a significant proportion of payments still being conducted by cards, the first thing retailers need to understand is that there are Payment Card Industry Data Security Standards (PCI DSS) requirements based on their footprint and volume. Effective partners come in and initiate risk descoping exercises, which effectively removes or minimises risks by implementing solutions such as point-to-point encryption for cards.

Naturally, cash is still highly prevalent in South Africa, meaning that retailers need clearly defined systems and processes for how they manage cash. Technology plays an important role here, where reconciliation software ensures that retailers have financial certainty and a single source of truth for all the tender types they accept, and not just card payments.

The card space is already highly regulated, but with increasing options for alternative payments, such as SnapScan, PayShap, and even Cryptocurrency, regulators will mandate security mechanisms and best practice. Retailers should appreciate that these are new and different technologies, and as such they come with new and different challenges.

Cyber criminals evolve at breakneck speed, and in any organisation there are vulnerabilities in code that can be exploited. It is non-negotiable to build robust in-house capability to stay ahead of trends or partner with specialists who can. For example, while not directly related to payments, South Africa is now one of the most targeted countries in the world for ransomware.

Retailers need to stay in control

Yet, despite needing to address vulnerabilities across all attack surfaces, the biggest risk for any organisation is its people, followed by processes that fail. Retailers should proactively invest heavily in staff training and education, as well as reactive security in the form of audits and controls, which – if effective – can help it identify problems quickly.

Retailers also need to stay on top of preventative controls and measures to prevent any unauthorised individuals accessing their systems. It is too late if a breach is detected only after the nefarious actor has entered the environment. An example of this would be workflows to terminate unauthorised access during onboarding and offboarding of staff. Another effective security strategy, which is made easy with modern, best-of-beed in-person payment solutions, is segregating duties to ensure that one individual never has complete control over a process.

It is evident that every time someone taps their smartphone or enters a voucher code, there are a host of highly complex systems and processes that are triggered, including encryption, payment rails, switching, settlement and reconciliation, among more. Security needs to be woven into every step.

While this really has been the source of many sleepless nights for those in charge of IT and security at mid-market retailers, the evolution of technology means this no longer has to be the case. As long as a smaller retailer sources a

partner with a long, proven track record in the enterprise space that can bring the same level of tier one security and functionality to smaller businesses in simple one-stop solutions, it has all but future-proofed itself and can confidently punch above its weight.

ABOUT THE AUTHOR

Wayne Steppe, Enterprise Architect & Bernard van Der Merwe, Information Security Officer at Ecentric Payment Systems