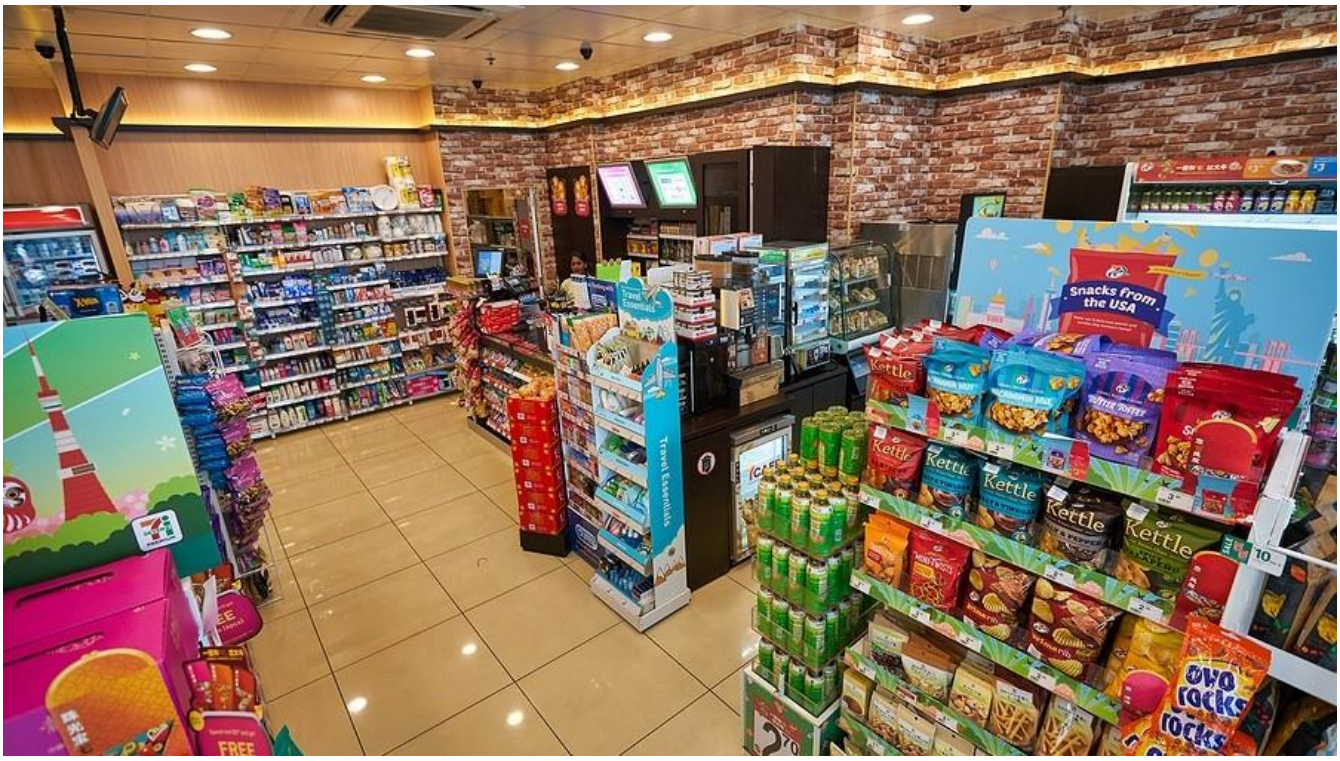
Retail Data Security Challenges Threaten Vulnerable C-Store Industry



In countless movies, harried convenience store clerks find themselves at the wrong end of an armed robber's gun. However, while armed robbery continues to pose a significant threat, a more silent digital danger costs the industry millions of dollars. Convenience stores must address retail data security challenges to protect themselves and their customers.

Cyber Criminals Love Convenience Stores

For cyber criminals, convenience stores represent an attractive target. On the one hand, c-stores collect a huge amount of valuable data. Between in-store purchases and outside fuel pump transactions, a single store processes hundreds, even thousands, of credit cards each day.

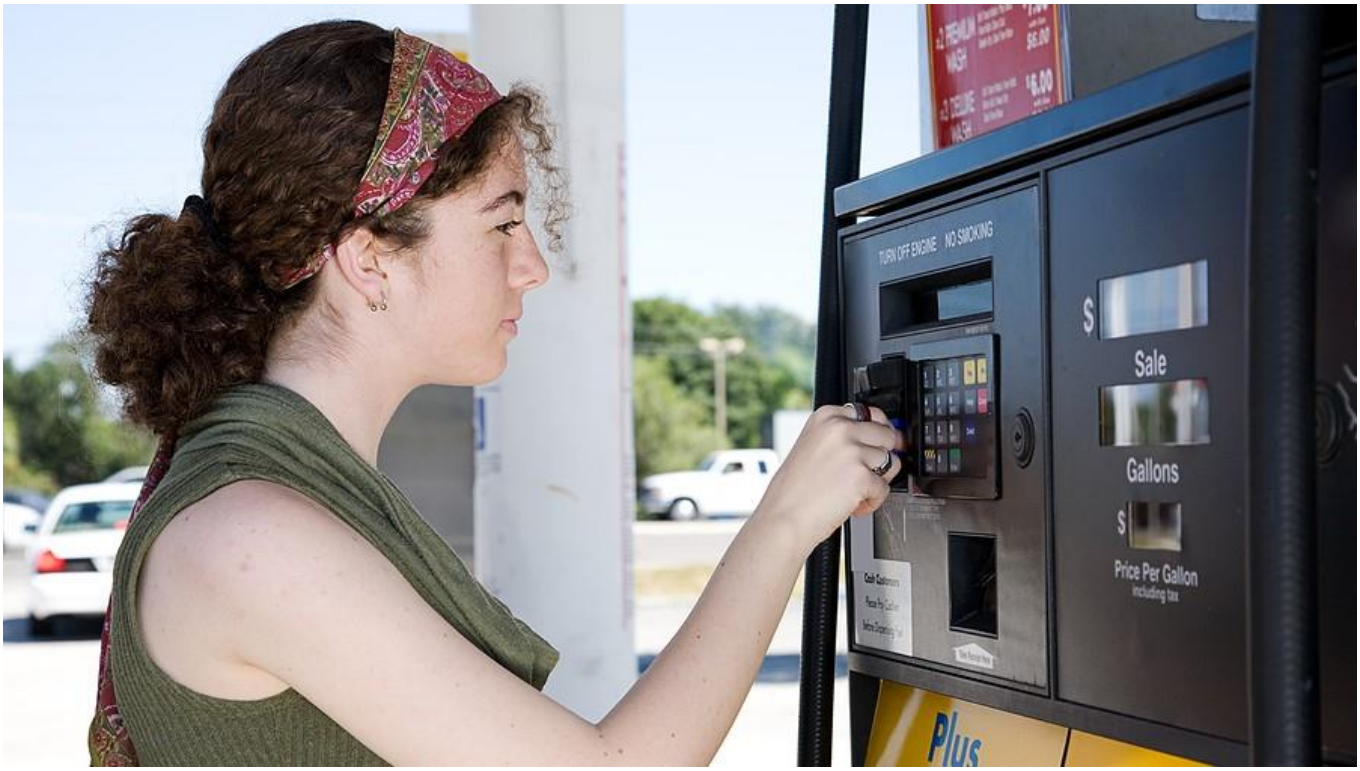
This treasure trove of data yields assets a cyber-criminal can both use and sell. For instance, a single credit card can bring from ten cents to one dollar on the black market. Thus, the stolen data from thousands of credit cards delivers a substantial payday.

Additionally, the c-store industry has not invested in cybersecurity to the extent that other industries have. Consequently, c-stores leave themselves particularly vulnerable with outdated technology and poorly trained staff.

Top Retail Data Security Challenges for C-Stores

Recently, the National Association of Convenience Stores (NACS) reported that payment security and data breaches represent the top c-store security issue. A closer look at the data security challenges faced by c-stores reveals several common themes.

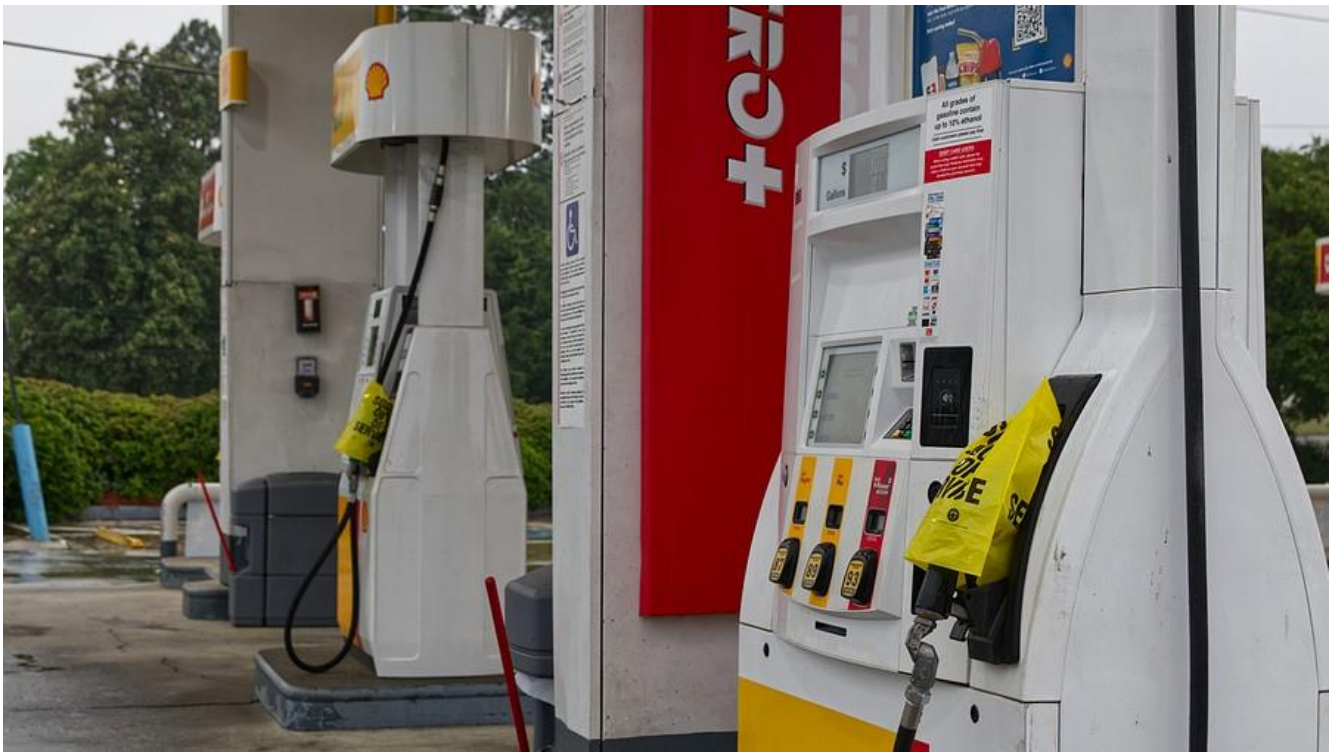
- **Card skimming at POS** – Fuel pumps have emerged as a common target for bad actors who steal credit or debit card information through a process known as skimming. With skimming, the thief installs a card-reading device on the fuel dispenser. And with employees busy inside, thieves can easily install the devices and steal customer data.



- **Achieving regulatory compliance** – Like most industries, the c-store industry must comply with a steadily increasing number of privacy regulations. And with the bulk of customers paying with credit cards, PCI DSS compliance plays an essential role in cybersecurity strategies.
- **Human factor complicated by work conditions** – In any industry, the human element represents a weak link. High turnover in the c-store industry compounds the problem. Additionally, employees often work alone, for long hours and late at night. This makes them particularly vulnerable to social engineering.
- **Insufficient cybersecurity investment** – While cyber criminals constantly deploy more sophisticated technology, convenience stores tend to lag behind. Stores utilize outdated hardware and software and delay implementation of critical security measures such as multi-factor authentication, encryption and adequate end-point security.

The Buck Stops…Where?

Statistics clearly show that data breaches pose a critical problem for convenience stores. But determining who owns the problem presents a challenge. Cyber criminals run their operations as big business, and they have the means and the expertise to devise increasingly sophisticated attack strategies. Single stores and small chains simply cannot keep up with the technology.



At the same time, the credit card industry has also fallen behind in technology innovation. Credit cards remain vulnerable, easily compromised. Even when defensive technology does exist, as in the case of EMV chip card technology, many stores delay implementation. Even customers fall behind in knowing the signs of card skimmers and other dangers.

Closing C-Store Security Gaps

Consequently, the solution to retail data security challenges must include multiple strategies. As a first step, c-stores should review cybersecurity policies and procedures. This is a good time to conduct a security and compliance risk assessment. Additional critical security steps include updating unpatched or outdated software and hardware and strengthening passwords.

Beyond these basic steps, c-stores strengthen cybersecurity by implementing EMV chip technology and leveraging automation. The retail IT experts at eMazzanti can conduct risk assessments and guide organizations through implementing a comprehensive data security strategy.