The Next Frontier of Security

In

Retail Petroleum

Thomas Park
VP Product Mgt, Gilbarco
A view of the bad guys

- Fraud follows the easiest paths
- As sites lock down with EMV, the rest become more vulnerable and TARGETS
- Total Fraud $ likely to increase in the near term -- hitting the sites that do not adopt

It is Imperative that you do not delay implementation of EMV – independent of the 2020 shift!
Traditional Threat Vectors for Retail Petroleum

1. Card swipe -- card data (EMV)
2. Communication to the store/FCC/POS – Cat5, OTW, Wireless (P2PE)
3. POS/BOS in store data (PCI-DSS)
4. Secure gateway site to WAN (PCI-DSS)

This is the Realm of EMV, P2PE and PCI-DSS
While the potential damage from traditional threats is huge – Disruptive threats are even bigger

Technology is moving crazy fast and the industry’s ability to keep up is challenged

IoT
Cloud
Data, Data, Data
Connected Car
To compete and win in today’s world of Amazon, Tesla and other new entrants ... You have to play in the cloud.

Need to join the game and change the rules where you can...
The new threat vectors...

1. Distributed Denial of Service Attack (DDoS) using all bandwidth and resources
2. Intrusion and data theft -- Penetration from site to HO – including Phishing attacks
3. Hijack of dispenser and forecourt payment– Man in the Middle
4. Non authenticated device connects to cloud Or V2I – penetration of Vehicle

Successful attack can lead to:
- Site shutdown
- Safety measures violated
- Damage to equipment
- Undetected spills
- Brand Damage
The new Counter Measures and Best Practices

- 2-Factor Hardware Based Mutual Authentication
  - Both sides trust who they are talking to

- PKI Certificate Swap
  - Both sides exchange protected information that is used to build a secure pipe

- TLS 1.2
  - Build a secure pipe through which information can be securely passed

- Certificate Replacement & Software update
  - Renew certificates frequently just in case someone figures out the protected information. Enable SW update to maintain latest versions
Summary

- Must move asap to lock down traditional threat vectors
- The cloud opens up your ability to compete in today’s world
- ....It also opens up new attack vectors
- A clear IT policy on intrusion detection with tight controls on authentication and access enables you to enter the playing field