

Security Guardian

Tom Kellermann, vice president of security awareness at Core Security and former head of cyber-intelligence and policy management at the World Bank, talks PCI compliance.

Q: What can retailers do to protect themselves from security breaches?



exploited by hackers. It is also important to move away from static passwords and implement more robust authentication solutions. Retailers should always be wary of their wireless deployment — their Achilles' heel. It should be encrypted and all MAC addresses and passwords changed regularly.

Q: How does the retail industry, and specifically the convenience industry, compare to others in adopting better security measures?

A: They are not in the lead. In fact, they trail behind other industries because many do not fully appreciate that they have become a target of choice for cyber-criminal

syndicates. The overt focus on physical security has created a cyber-security quagmire. Many retailers are far too over-reliant on encryption for information security and assume if the data is encrypted they will be secure — this is a myth. The private keys that unlock the cipher are stored on computers and can be stolen by hacking that device and thus unlocking the encrypted data, leaving the store's network naked.

A: Retailers should come to the realization that the biggest threat to their profit margin is no longer the shoplifter but rather a virtual thief who can empty their customers' bank accounts and steal their identities. In order to prevent this dire phenomenon, retailers should maintain up-to-date network topology diagrams and conduct penetration tests of known IT assets on a quarterly basis to discern weaknesses before being

Q: What new technologies are making retailers more vulnerable?

A: Retailers have become significantly more vulnerable due to the overt use of wireless and the remote deposit capture scanners that exist at point-of-sale terminals.

Q: Do you expect retail industry security breaches to increase in the coming years?

A: I do — by a factor of ten — as criminals have begun to recognize that money is digital and retailers have become quasi-banks due to the amount of financial data they process and store. Retailers are easier to hack than banks and thus many cyber-syndicates will focus their attention upon them.

Q: Why do you think many companies are delaying becoming PCI compliant?

A: Lack of PCI compliance is due in large part to ignorance. I believe that many lack the respective leadership such as a chief information security officer or director of security who has an IT background versus the common physical security background.

Q: What can you say to encourage retailers to become PCI compliant?

A: The first movers toward PCI compliance will experience far less operational and reputational risk. Being PCI compliant is akin to having closed circuit cameras, alarms, tags on goods and security guards in the physical world. The hacker community will choose less secure retail targets before the hardened targets. ■