□□□□□□□□□□

WHITE PAPER

How to simplify and control the cardholder security environment

Document Version V1-0

Document Set: QCC Information Security

Prepared By Nick Prescot - QCC Information Security Ltd

Sponsored By Mako Networks Ltd

TAKING THE BITE OUT OF PCI DSS COMPLIANCE

How to simplify and control the cardholder security environment

Small card-present merchant sites can be costly and time consuming to make PCI DSS compliant. Many businesses do not understand the full requirements of PCI DSS, and when it comes to self-certification, many small companies are more concerned about taking payments than implementing the security controls demanded by PCI DSS.

Scenario

A merchant finds out through his acquiring bank and card scheme that a security breach has been traced back to his business. Fraudulent transactions had been occurring over the last 12 months, and his site was responsible.

The fraud happened because the merchant had a poor understanding of the PCI DSS security requirements, and lacked proper security controls needed to prevent an intrusion. As a result of the breach, the merchant was fined £10,000 by the card company and had to pay the cost of the investigation: a further £20,000.

In addition, the merchant was instructed to attain PCI DSS Level 1 compliance within 90 days, adding another £20,000 to the sum owed. The Data Protection Commissioner ordered the merchant to notify all his affected customers, resulting in a 40% drop in business over the next six months, as customers no longer trusted the organisation.

This is an actual scenario that QCC dealt with as part of an investigation in the last 12 months, and evidence that PCI DSS non-compliance can cost merchants dearly.

Fraud payments – who picks up the tab?

For cardholders, fraudulent credit card charges are usually reimbursed fully and the compromised card is cancelled and re-issued. Though the card has been used for fraud, a cardholder is not responsible for the financial loss of that crime. For merchants and banks however, the fines and financial penalties from card fraud and data breaches are increasing dramatically.

Merchants most often bear the financial burden of card fraud crimes, laden with the cost of required forensic investigations because they were not compliant with security standards. The acquiring banks meanwhile have to cover the overall loss and recover the funds.

Research shows that credit card fraud is a growing problem, and increasingly targeted toward smaller merchants (Levels 3 and 4 as defined by the card schemes), or the smaller satellite locations of larger companies. Recent evidence has shown that 96% of PCI DSS security breaches happen with Level 4 merchants.

Most card fraud is perpetrated by criminal gangs with sophisticated means of compromising basic security.

Prevention is better than cure

The most sensible way to implement and measure effective PCI DSS compliance is to utilise a solution that delivers maximum control to the acquiring bank or service provider, while requiring minimum effort from the merchant.

Acquirers strive to meet their obligation to the card schemes and ensure their merchants are compliant. A common first step for small merchants is to create a compliance program supported by an online self-assessment portal. While this is an easy and appropriate first step, merchants often tick the appropriate boxes without any certainty that they actually meet the requirements, and seldom have detailed knowledge of their computer and payment network configuration. Even if the self-assessment questionnaire is completed correctly, it is imperative that merchants be compliant at all times, not just at the time of audit or self-assessment.

Acquirers are still liable for fines if forensic investigation determines that the PCI DSS standard was not correctly implemented. Typically, the first time an acquirer discovers a merchant is not compliant is when it's already too late, and the card scheme has notified the acquirer and merchant of a breach.

Dial-up vs. IP networks

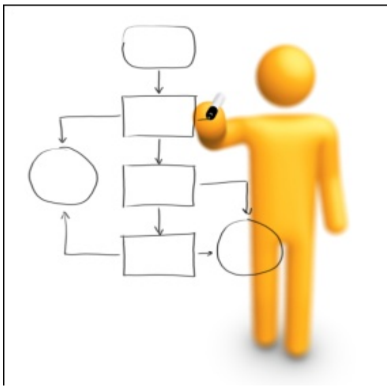
Many small and large merchants use dial-up Internet connections to process the payments from their PIN Entry Devices (PEDs), but the future of this method is limited. While consumers have moved from dial-up Internet services to broadband, with increased speeds and reduced costs, the payment industry has lagged behind. These same speed and cost benefits are needed by merchants of all types to process transactions. Using broadband, merchants can ‘queue bust’ during busy periods, reduce costs by consolidating phone lines and link with Enterprise Resource Planning systems and resources.

Many companies are wary of moving to a high-speed Internet Protocol (IP) network because of the implications it may have on PCI DSS. If companies add IP-compatible PEDs to their network, it immediately brings a company’s entire network into the scope of PCI DSS, adding complexity in attaining compliance and increasing risk.

For acquiring banks, switching to IP networks allows the costs of dial-up connections to be reduced or removed completely.

While merchants carry the monthly cost of the phone lines for dial-up connections, banks will typically pay for the costs of each dial-up call and transaction. Therefore, the benefits for both banks and merchants to drop the costs associated with dial-up are very compelling.

In 'multi-lane' environments like a grocery store, for example, where there is a requirement for many payment stations and PEDs, the cost of individual dial-up connections can quickly add up, while a single IP network connection costs far less.



Another problem with dial-up transactions is the speed of service. Customers often become frustrated waiting for card payments to be accepted and cleared at the point of sale. When people want to make purchases quickly and easily, queues at the checkout may send them elsewhere.

IP network compliance

One of the goals of PCI DSS is to ensure that the Card Data Environment is separated from open IP networks and protected by firewalls.

Cardholder data needs to be protected from the rest of a merchant’s IP network. If it's not, the likelihood of a breach increases dramatically. Controls and procedures mandated by PCI DSS ensure that separate networks are used to create a safe cardholder environment.

For most merchants, cost is very important when considering PCI DSS compliance. While on a dial-up network, they're exempt from PCI DSS networking requirements. But despite the exemption PCI DSS challenges, broadband IP networks still represent a proven, reliable, low cost alternative to dial-up if it can be appropriately secured. However, the complexity of achieving and maintaining compliance has stymied widespread adoption of these networks.

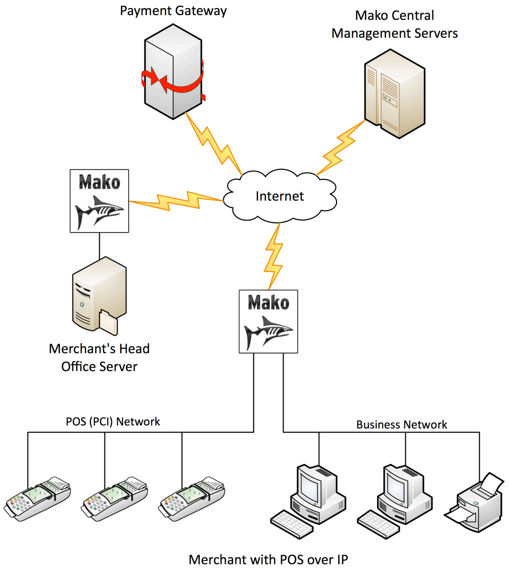
A PCI DSS solution that uses public broadband has been long overdue. Products and services from Mako Networks make this achievable and address all of the networking security aspects of the PCI DSS standard. Customers that have implemented this solution have significantly reduced the complexity and cost of meeting PCI DSS.

The Solution

While there is no ‘silver bullet’ solution for PCI DSS compliance, there is a solution that makes most aspects of network security easy.

Mako's PCI DSS solution was developed after contact from a telecommunications corporation that wanted a less expensive and simpler way for its customers to achieve PCI DSS compliance.

Mako Networks' solution simplifies and streamlines the requirements to meet PCI DSS. The diagram below shows how the system physically separates the networks to reduce the risk of fraud at merchant sites.


Payment Gateway
Mako Central Management Servers
Mako
Internet
Merchant's Head Office Server
Mako
POS (PCI) Network
Business Network
Merchant with POS over IP

Most small merchants do not have in-house information security specialists, let alone an accredited PCI Qualified Security Assessor. Larger merchants with numerous small retail sites face a similar challenge. While they typically have access to capable technical teams, the expertise is centralised at main locations, and the impact of having to manage hundreds of remote sites to the level required by PCI DSS is huge.

Giving merchants a single pre-configured and remotely managed security appliance which continually enforces compliance to replace traditional modems, routers and firewalls dramatically simplifies the self-assessment and audit process for merchants.

A key advantage of the Mako solution is that merchants are not tied to a specific Internet service provider. Mako allows the merchant to use any provider they wish for broadband service.

Mako's unique selling point is that investment in infrastructure is not required, and the solution is instantly deployable.

In regards to PCI DSS, compliance is instant with the Mako Networks system, and that compliance is maintained and measured in real time.

Investment in a solution that separates the network at the physical layer ensures that merchants attain a more mature level of compliance.

How does Mako assist Level 1 merchants?

In a scenario with multiple sites that need to achieve compliance, a traditional solution that might look simple can prove costly to implement and complex to configure and control. There is also a very real risk that it will fail to meet compliance standards or require repeated costly physical site visits to maintain compliance.

With the Mako Networks system, all the end-points are centrally configured and managed from a Central Management System (CMS). Any changes to the network environment are centrally approved, significantly reducing complexity and provisioning costs.

Another advantage of the Mako Networks system is that a merchant's existing IT infrastructure can be used without major disruption. Mako hardware fits into an existing network and does not require a separate networking system.

For many small-site merchants, there is a great deal of complexity and confusion over PCI DSS implementation. But by using a new or existing broadband connection with the Mako system, a small-site merchant can implement a fully compliant solution quickly and easily.

The Mako system can be integrated with any Ethernet-capable Point of Sale system or payment terminal.

Using the Mako Networks system, the merchant's PCI DSS self-assessment questionnaire can be reduced by up to 90%, saving time and increasing the response accuracy for the remaining questions.

Preventing terminal manipulation

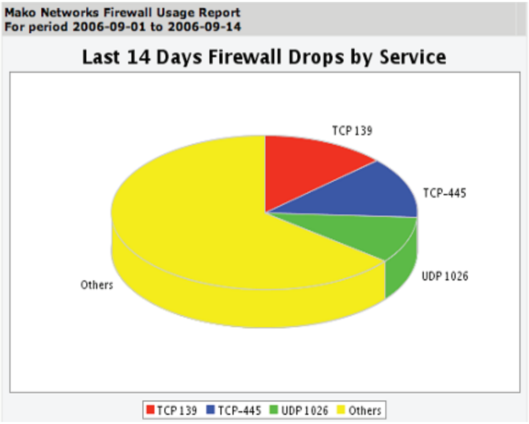
Terminal manipulation describes a situation where someone removes, changes or introduces a 'rogue' PED into a payment system to steal card information. Typically, this rogue PED will include malicious software that records and sends card data to a criminal gang that can then on-sell the information for a profit.

The Mako solution requires that PEDs are registered via the CMS, ensuring that terminals cannot be removed or introduced without pre-authorisation. Furthermore, the system will only allow the registered PEDs to communicate with approved payment 'gateways', mitigating the risk of payment requests being misdirected to the criminals.

Simplifying the auditing process

Auditing is vitally important to any business, whether it be from an external perspective or a management overview. The Mako system can be audited by both the acquiring bank and business management, providing assurance that the merchant's networks are maintained in a PCI DSS-compliant manner and reducing the risk of a security breach.

Should a breach be suspected, merchants are able to display a real-time status log of compliance. As long as there has not been an unauthorised change to the network setup--which the Mako system can prevent--it can be quickly ascertained that PCI DSS compliance has been maintained.



If the source of a suspected security breach can be determined quickly and accurately, some card brands and acquiring banks may not require a remedial action from an external party. Since the Mako system monitors in real-time, any incidents are tracked and identified immediately.

Benefits for the acquirer

One of the most significant challenges for acquiring banks is ensuring that small merchants are PCI DSS compliant. Very few merchants are information security experts, and most consider a Qualified Security Assessor audit or the cost of a forensic investigation to be an unnecessary cost. Instead, many merchants choose online certifications that require minimal auditing of their systems in the mistaken belief that this alone meets the requirements of PCI DSS.

The Mako Networks system gives the acquirer a real-time picture of compliance, rather than relying on merchant self-certification and the possible consequences.

Complying with PCI DSS can be complex, and requires capital investment when a card-present merchant moves from a basic 'dial-up' environment to a faster and less costly IP network connection.

Present compliance solutions require complex networks to ensure that the cardholder environment is separated from the rest of business. These are often expensive and difficult to maintain.

Implementing an IP-based solution like one from Mako Networks that is PCI DSS compliant at minimal cost is not only a technological breakthrough, but also a business breakthrough.

About QCC

QCC are leaders in the field of Incident Response. As a dedicated professional information security company, QCC provides expert services around:

1. Incident Response
2. Incident Management Training (generic and QFI)
3. Audit and Compliance (PCI, ISO 27001, CoBiT, BITS and many other areas)
4. Penetration and vulnerability testing
5. Digital and Mobile Forensics

QCC also develop Blackthorn, a fully in-house developed GRC activity management application.

Visit www.qccis.com/blackthorn for more information.

About Mako Networks

Mako Networks is the leader in secure router and network management technology. By using innovative technology and segregated networks in their routers, Mako is able to offer new solutions for:

- PCI DSS compliance
- Secure Web Access control
- Mail Sanitisation
- Real-time network traffic management
- Automated security system updates
- Centralised network control

Mako Networks is headquartered in New Zealand with offices in the UK, Australia and Bahrain.

Visit www.makonetworks.com for more information.

Glossary

PCI DSS	Payment Card Industry Data Security Standard
PCI-QSA	Payment Card Industry Qualified Security Assessor
Acquirer	Company that takes and processes credit card transactions
SAQ A/D	Self-Assessment Questionnaire levels A-D
PED	PIN Entry Device
CMS	Central Management System