Advanced guard

The target-rich gaming industry needs to think seriously about data security in order to avoid bad publicity and lost revenue, says CardConnect Payments Executive Vice President **Scott Dowty**

We see it in the news almost every day: Despite being PCI (Payment Card Industry) compliant, a company or a government agency has been breached, putting millions of financial records and personal data into the hands of hackers and ultimately, on the black market. The gaming industry is a high profile, payment transaction-rich environment living on borrowed time. With last October's adoption of EMV (Europay, MasterCard and Visa) and its credit and debit chip cards in the USA, card-not-present (e-commerce/online) fraud will likely increase dramatically over the next three years, as evidenced in European countries, following wide EMV adoption.

When it happens in the gaming industry, and according to experts it will, who will pay for it? Lisa Monaco, US Homeland Security advisor to President Obama, stated, "There are two types of merchants in this arena; those that have been hacked and those that will be hacked." There may be one more type; those that have been hacked but are unaware yet. Bad publicity and a loss of consumer trust come standard with a large data breach, but there is also the financial impact, which could amount to thousands or millions of dollars lost.

Many customer service centres were in operation long before PCI standards were established, and there is a myriad of contractual structures as to where the liability might lay. In some instances, the entire operation is outsourced to a service provider; in others, the organisation performs all services. Several variations of these two scenarios exist where a casino might outsource a portion while using a software application from a large systems integrator. It is worth considering if all of the existing contracts are aware of today's environment and the associated risk.

Experts agree, however, that payment security is being challenged in the gaming industry.

FIVE CRITICAL LEVELS OF SECURITY

The surest way to protect sensitive data, such as customer credit cards, personally identifiable information and player data is to remove as much of the sensitive information from the merchant's environment as possible, often referred to as taking the merchant out of PCI scope. If the information does not touch the merchant's system, there is no valuable data to steal. There is also the opportunity to avoid the costs associated with becoming PCI compliant and maintaining compliance, as well as avoiding risk to the merchant's brand and eliminating financial penalties.

The steps to achieve an out-of-scope environment are as follows:

PHYSICAL DEVICE SECURITY FOR CARD-PRESENT

In many breaches, the systems is compromised by malware installed on point-of-sale (POS) systems. Criminals use skimming devices to grab credit card information – even wirelessly with Bluetooth . PCI 3.0 has stricter standards for maintenance, including documenting all devices and their unique identifiers, and inspecting those devices regularly.

SECURITY FOR CARD-NOT-PRESENT (ONLINE AND CSC TRANSACTIONS)

With the rise in fraud, the PCI Council, which is the self¬ governing arm of the Payment Card Industry, adopted additional security measures. One security measure is the creation of the PCI's Point-to-Point Encryption (P2PE) certification. A P2PE solution secures sensitive data from the point of interaction all the way to the completion of a transaction, and is one of the safest options for protecting payment data.

TERMINAL TO GATEWAY TRANSMISSION

As sensitive data moves from the terminal or network into the gateway, there are instances when data is unencrypted; for example, when card data leaves the merchant network. While the move to EMV cards will mask this data with computer chips, the only way for a business to truly protect itself is to encrypt data at the point of interaction (POI).

GATEWAY TO BANK TRANSMISSION

PCI standards require payment gateways to transmit data to a select list of certified processors' IP addresses. At this point, data leaves the merchant's system and carries inherent vulnerability because it must be unencrypted before reaching the bank or processor. Payment gateways must halt data transmission to foreign IP addresses outside of that list.

STRICT NETWORK MONITORING/ VULNERABILITY MANAGEMENT PROGRAM

PCI DSS (the Payment Card Industry Data Security Standard) requires merchants to

regularly track and monitor access to network resources and cardholder data, and regularly test security systems and processes. Without proper follow-through, a data breach is likely. PCI3.0 includes a new section that provides guidance for implementing security measures into 'business as usual' activities to maintain compliance.

ACHIEVING PAYMENT SECURITY

A true P2PE solution, certified by the PCI Council, encrypts card data at the point of entry so the merchant cannot decrypt it. The data stays encrypted until it reaches a hosted environment. Merchants benefit tremendously from P2PE solutions – most notably, PCl -certified P2PE solutions reduce PCl requirements.

CONSEQUENCES OF A DATA BREACH

The effects of a security data breach are far reaching and can have substantial negative impacts on a company or organisation of a hosted environment. Merchants benefit tremendously from P2PE solutions – most notably, PCl-certified P2PE solutions reduce PCl requirements.

There is a difference between P2PE and end-to-end encryption (E2E). E2E solutions do not provide the same PCI compliance benefits, nor have they been subjected to PCl's rigorous certification process. Only those solutions listed as P2PE on the PCI Council's website are true P2PE.

The purpose and goal of the EMV standard is interoperability between EMV cards (also known as chip cards) and EMV-enabled payment terminals throughout the world. There are two major benefits associated with chip-based credit card payment systems; improved security (with associated fraud reduction) and more control over offline credit card transaction approvals.

It is significantly more difficult and expensive to replicate EMV cards than magnetic stripe cards. As of October 2015, a merchant using a terminal without EMV capability is liable for any fraudulent transactions if the victimised customer uses a chip card. While this is a major step forward in the quest to control breaches, EMV alone is not enough to keep data safe, in fact it does not protect card-not -present transactions. The ideal solution is a combination of tokenisation, P2PE and EMV.

Tokenisation has reduced the scope of PCl DSS requirements for many organisations, especially online (e-commerce) environments, by sanitising sensitive data in the end-user's browser before the payment is submitted. When a customer enters a card number, it is sent to a securely hosted vault and a token is delivered to the customer's computer. By tokenising the card number on the checkout page prior to the card number entering the web environment, the entire website is removed from PCI scope. There are two methods of using this type of tokenisation technology: the tokeniser can be embedded into specific fields on a website using an iFrame or a payment page is fully hosted by a third party (called a hosted payment page). There are configurations available to keep a hosted payment page consistent with the organisation's website and branding, or you can choose to pre-populate the fields if the customer information is already on file.

A Ponemon Institute study shows that the business impact of a data breach is detrimental in many ways, including the up-front costs of notifying each affected person. The investigation and controls that need to be put into place, and litigation may result in US$217 per compromised record. It's simple math: one million records breached (representing a medium-sized gaming entity) equals US$217M in costs. The long-term effects include damage to the brand and loss of trust, loss of customers and negative political implications. ◄

Scott Dowty is executive vice president for CardConnect Payments. He is based in Las Vegas, Nevada, USA