WHITEPAPER

PCI Compliance:

Protect Cardholder Data with Advanced Redaction

By Troy Burke

extract

WHITEPAPER

PCI Compliance:

Protect Cardholder Data with Advanced Redaction

By Troy Burke

Is PCI-compliance on your IT priority list?

Organizations accepting credit and debit cards as a form of payment have a responsibility to protect customers' card information. The Payment Card Industry (PCI) plays an important role in the regulatory compliance environment protecting this sensitive content. Despite the fact that there are numerous technology providers in the security market that help with PCI-related compliance initiatives, a recent survey by Gartner found that 18 percent of respondents admitted to not being PCI-compliant.

What is PCI and who must comply?

> *“Despite the fact that there are numerous technology providers in the security market that help with PCI-related compliance initiatives, a recent survey by Gartner found that 18 percent of respondents admitted to not being PCI-compliant.”*

The Payment Card Industry Security Standards Council (PCI SSC) is an organization founded by American Express, Discover, JCB International, MasterCard and Visa. It was formed to govern the security of sensitive cardholder data. The Council developed the PCI Data Security Standard (PCI DSS); a worldwide information security standard which contains the requirements merchants must follow to protect customers. The PCI DSS applies to all entities, large and small, including government agencies, that process, store, or transmit cardholder data. The first version of PCI DSS was introduced in September 2006. At this time, the PCI Security Standards Council (PCI SSC) established a continual two-year cycle of review and revision.

Merchants fall under four categories of PCI compliance, depending on the number of transactions they process each year, and whether those transactions are performed from a brick and mortar location or over the Internet. Failure to maintain compliance with the PCI DSS puts your organization at risk of significant fines, fees, penalties and losing the ability to process card payments. What's more, a suspected or known compromise of your card processing systems can result in serious damage to your organization's reputation and potential litigation brought by impacted cardholders and issuing banks who suffer losses as a result of compromised information.

...continued page 2

> “By blocking sensitive content from unprivileged viewers, redaction helps organizations meet compliance mandates while gaining efficiencies through the automation of data protection.”

The PCI DSS are broken down into 6 categories. Each has various sections and associated requirements:

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software on all systems commonly affected by malware
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

PCI-compliance is perhaps more misunderstood than difficult. In fact, many respondents in the Gartner survey said they were taking steps to improve their abilities to meet PCI-compliance guidelines, and cited Security Information and Event Management as one of their most pressing IT priorities.

Private and public sector organizations are using automated redaction technologies to meet PCI-DSS compliance requirements for protecting cardholder data and restricting access. Redaction is the permanent removal of sensitive information from electronic documents. By blocking sensitive content from unprivileged viewers, redaction helps organizations meet compliance mandates while gaining efficiencies through the automation of data protection.

...continued page 3

ID Shield Advanced Redaction from Extract Systems supports PCI-DSS requirements by automatically identifying and protecting sensitive data in structured (forms) and unstructured documents. Using state-of-the-art data detection capabilities, ID Shield supports the redaction of CVV (three-digit security code), credit/debit card numbers, expiration dates, account numbers, check numbers, medical information and virtually all types of sensitive content and personal information.

Author:
Troy Burke is the
Director of Government Solutions
at Extract Systems.

Extract Systems *is a leading provider of advanced data capture and redaction solutions that drive operational efficiency and secure private information for government, healthcare and other commercial sectors.*

ID Shield's ability to detect and remove sensitive data in structured and unstructured documents is driven by advanced logic that incorporates pattern recognition, phrase context, proximity and keywords. This robust data security software has processed more than 1.5 billion documents for over 500 customers without a single breech in data protection. Extract's data capture products automatically find and incorporate manual data entry fields into designated information systems as structured data. Automating the capture of information trapped in paper-reliant workflows reduces costs and optimizes the intelligent collection of data.