

MEMBER SPOTLIGHT

PEGASUS TECHNOLOGIES: SECURING AND MANAGING YOUR DIGITAL WORLD



Matt Tucker; VP of Pegasus Technologies

On April 30 of this year a set of requirements for enhancing payment account data security developed by The Payment Card Industry Security Standards Council (PCI) will be enforced, impacting any company accepting payments via credit card. Even businesses that conduct just a few credit card transactions each year will be held accountable for meeting the standards. Fines for non-compliance can be levied for as much as \$500,000.

“Organizations may know what is at risk, but to make sure they’re getting the message, government and watchdog organizations are setting stringent standards that hold the company, as well as its executives, personally responsible in the case of a security breach,” says Matthew Tucker, Vice President at Pegasus Technologies based in Media, PA. “The cost of fraud is enormous, and it is only going to get worse if proper security is not in place.”

Major incidences of data theft in the past several years have indeed been costly in both dollars and organizational credibility. As reported, a security breach at TJX, the Massachusetts-based retailer that operates T.J. Maxx and Marshalls, exposed over 45.6 million credit and debit card numbers, resulting in numerous lawsuits and heavy fines.

T.J. Maxx is big news, but most small business compromises go unreported for many reasons like fear of bad publicity or the thought that law enforcement couldn’t help. The truth is Small & Medium businesses have a great risk due to their lack of in-house knowledge, antiquated hardware & software solutions and loser data security policies, if any.

Among the requirements to be enforced for security management are: installing and maintaining a firewall configuration to protect cardholder data; encrypting transmission of cardholder data across open public networks; developing and maintaining secure systems, applications and assigning a unique ID to each person with computer access; regularly monitoring and testing networks; and a requirement to maintain a written formal policy to meet these objectives.

These aren’t the only data security standards businesses, no matter how large or small, are expected to meet. The Health Insurance Portability and Accountability Act (HIPAA) has changed the legal and regulatory environments governing health care and the Sarbanes-Oxley Act makes CFOs fully accountable for all of their companies’ financial data.

“Today’s internet access can allow a hacker to touch almost any computer in the world,” says Tucker. “Organized crime has become more sophisticated in the buying and selling of credit cards and social security numbers.”

Tucker and his colleagues started Pegasus Technologies in 1998 with an objective of helping companies of all sizes manage and remediate security risks. Pegasus has become a market leader in IT-based security solutions, and its Risk Management Division (RMD) specializes in security assessments and the design and implementation of security systems.

“Our RMD can expose vulnerabilities in your company’s network and help you address them based on the latest compliance regulations,” says Tucker. “With the new PCI regulations, any company that takes just one credit card transaction a year should at least talk to us.”

In addition to security services, Pegasus Technologies offers a full range of professional services such as desktop and server support for Windows, LINUX and MAC, backup services, managing of e-mail and network design and implementation services.

For more details about Pegasus Technologies please visit their website www.pegasustechnologies.com. To speak with someone directly, feel free to call 484-212-4048. A representative is available during normal business hours as well as 24/7 emergency support.

The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the 64 DSS requirements are organized into the following categories:

BUILD AND MAINTAIN A SECURE NETWORK

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

MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

- REQUIREMENT 5: Use and regularly update anti-virus software
- REQUIREMENT 6: Develop and maintain secure systems and applications

PROTECT CARDHOLDER DATA

- REQUIREMENT 3: Protect stored cardholder data
- REQUIREMENT 4: Encrypt transmission of cardholder data across open, public networks

IMPLEMENT STRONG ACCESS CONTROL MEASURES

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