IT Governance urges US stores to strengthen their levels of cyber security

IT Governance is urging US stores to strengthen their cyber security levels after fears of data breaches increases.

BOISE, IDAHO, USA, May 1, 2014 /EINPresswire.com/ -- IT Governance, the single-source provider of cyber security solutions across America, is urging US stores to strengthen their cyber security levels after fears of data breaches increases.

In recent months, well-known US brands have been the victim of multiple cyber attacks, which have affected millions of customers nationally. Texas-based arts and crafts chain, Michaels Stores, is the latest in a string of organizations to be breached. It was confirmed on April 17 that 2.6 million card details had been stolen which included customer information such as payment card numbers and expiration dates.

This breach follows the infamous attack on Target which affected 40 million debit and credit cards in December 2013.

Founder and Executive Chairman of IT Governance, Alan Calder, is encouraging businesses to take action: “These breaches should really be making US stores across the country sit up and take note. Too long have organizations prioritized infrastructure cost ahead of risk to their customers and this has got to stop. How many more breaches will it take for organizations to put precautions in place? Don’t wait until it’s too late; act now.”

Whilst it is mandatory for many organizations across the world that process, transmit or store payment card information to be compliant with the Payment Card Industry Data Security Standard (PCI DSS), it is not required by federal law in the United States. There are also no laws enforced by the US Government to help strengthen cyber security levels of businesses and organizations across America as a whole.

IT Governance is calling US stores, and those that deal with sensitive customer information, to be pro-active in securing their confidential data by putting appropriate measures in place before a breach occurs. Complying with the PCI DSS and implementing an Information Security Management System (ISMS) that is aligned to ISO27001 (recognised worldwide as the cyber security standard) are renowned methods for significantly strengthening an organization’s level of cyber security.

Documentation toolkits from IT Governance Publishing (ITGP) are a straightforward solution for many businesses who are looking to strengthen their cyber security levels. The toolkits have been developed by cyber security experts to provide policies, templates, checklists and pre-written, customisable documentation that can make implementing cyber security frameworks simple and easy to maintain.

Find out more:

PCI DSS v3.0 Documentation Toolkit: www.itgovernanceusa.com/shop/p-1011.aspx
ISO27001 2013 ISMS Standalone Documentation Toolkit: www.itgovernanceusa.com/shop/p-1382.aspx

Melanie Watson
IT Governance
448450701750
email us here

This press release can be viewed online at: http://www.einpresswire.com

Disclaimer: If you have any questions regarding information in this press release please contact the company listed in the press release. Please do not contact EIN Presswire. We will be unable to assist you with your inquiry. EIN Presswire disclaims any content contained in these releases.