The PCI Challenge

Michael Peters | August 29, 2011

It is frequently in the news. Reports have been written. Punitive and compensatory damages have been awarded. Companies around the globe have been challenged to find the resources required to comply with the Payment Card Industry Data Security Standard (PCI DSS). The prime PCI DSS objective is to protect cardholder data. The prime objective of all companies is to thrive in this global economy. The challenge is to remain ahead of the competition and the cyber-criminals who both want to take your hard earned resources away from you.
The price of neglecting business security might just be your business itself. Companies not only have to embrace the new PCI DSS policies and implement changes to policy, corporate culture, systems, applications and infrastructure, but they must also ensure that the solutions implemented achieve the goal.

In the case of PCI, it is your commerce solution exclusively. To accomplish this task, Companies must start with the right subject matter experts who implement the best of breed progressive solutions that include all retail touchpoints – in store, over the web, through call centers, via mobile devices and more. This commitment must follow thought the whole lifecycle of the technology initiative.

Consider the following analysis*:

- **302 million** customer records were compromised last year.
- **79%** of companies subject to PCI DSS whose records were compromised had not achieved compliance.
- **96%** of breaches were avoidable through simple or intermediate controls.

It is painfully obvious that security threats to retail organizations leave little margin for error. Retailers face increasingly complex security challenges – persistent threats that can undermine the success and longevity of a retail brand. Data protection, transaction security and compliance are just some of the high-stakes challenges retailers must address head on – particularly in a cross-channel commerce environment.

Many retailers struggle to:

- Prevent data breaches and keep the company out of news headlines.
- Minimize costly system downtime due to security issues.
- Achieve, maintain and demonstrate compliance and avoid penalties.
- Manage security with improved visibility, control and efficiency.
- Align security with the business to truly reduce risk and improve sustainability.

To address complex challenges, your retail enterprise security must incorporate constantly evolving technologies and technical disciplines. Recruiting, hiring and retaining qualified security subject matter experts to stay ahead of this create its own hurdles many organizations struggle with. One of the biggest challenges the world faces is that unqualified people make information security decisions. Part of this conundrum is a result of inadequately trained and skilled security practitioners while another part of the problem is technically challenged leaders who see security as a cost center rather than a competitive advantage. A business person would not approve a project or initiative that does not produce a return on investment, right? Avoiding risks satisfies this requirement from an opposing point of view. In simple terms, no data, no business. The CFO can say goodbye to the balance sheet if the company dies a catastrophic death due to the complete loss of intellectual property. A company makes money from competitive advantage.

When making security decisions, enlist the advice of qualified professionals. Consider not only depreciation and capital expenses, but also business continuity or disaster recovery expenses. These are fundamental risk management principles every security professional, business leader and government representative should be knowledgeable in.

** 2010 Verizon Business Data Breach Investigation report.*