



PCI Compliance: Shackles or Launch Pad?

Last Updated: June, 2010



Introduction

In 2006, the Payment Card Industry (PCI) Security Standards Council (SSC) was founded by the leading payment card brands. It developed the Data Security Standard (DSS) as a single set of requirements for enhancing the security of payment account data. Any organization that stores, processes or transmits cardholder data is required by contractual obligation to be compliant with the DSS.

As such, PCI compliance is often perceived by some organizations as something that is a valueless and externally mandated one-time activity. To many it is a burden, consuming resources they would rather spend on other efforts. At the same time, many other organizations have effectively launched security programs around DSS or have expanded their security programs using DSS. So which is it: shackle or launch pad?

Perception is Reality

Perceptions of a valueless effort are counter-productive and lead to the real-life consequence of minimal effort being invested in obtaining and maintaining PCI compliance. The larger consequence is that cardholder data is placed at unnecessary risk as a result of the minimal effort investment. In an organization that accepts credit card information, this minimal approach violates an implied trust that consumers have about their data being safe and protected.

Externally Mandated?

A child is given responsibilities to help him learn and grow and become a responsible adult. If the child shirks his responsibilities then rules and consequences may be attached as a means to help him learn and keep him safe.

This has been the case in the payment card industry. PCI compliance is the result of organizations (that store, process or transmit cardholder data) being irresponsible with regard to information security. Corporations have chosen profit over security and as a result, rules and consequences have been put in place. It is true that PCI has been externally mandated but if we tear down the wrapper and look closely, organizations have brought it on themselves by not making security a higher priority.

PCI Compliance as a Project

Most IT-related tasks, high priority or low, are considered one-time projects: install a server, upgrade a network, etc. With this mindset prevailing, it is no surprise that PCI compliance gets lumped in with these one-time tasks. The consequence of "PCI compliance as a project" is the minimal approach described above.

Validating PCI compliance happens as a snapshot in time. Things change in networks and systems all the time. Some of these changes affect an organization's compliance status. Without incorporating the data security principles associated with PCI compliance into the daily operations

of the organization, it is very likely that it will drop out of compliance and put cardholder data at risk in some way. One-time proof of minimal compliance does not mean an organization's data or its customers' data is secure. Data security is only achieved and maintained by long-term, consistent and focused efforts.

The Value of PCI Compliance

Chances are that the organization which takes PCI compliance seriously is an organization that is already mature with respect to security. However, for an organization that lacks compliance maturity, PCI compliance is no doubt a good start. The true value of PCI compliance comes with an organization's long-term, consistent and focused efforts towards information security.

In as much as PCI compliance applies only to the parts of an organization's network that store, process or transmit cardholder data, it is not a complete security program. There is more to information within an organization that is valuable and needs to be protected. The principles of data security associated with PCI compliance can be of benefit generally in an organization not just within the context of PCI.

PCI Data Security Standard as Launch Pad

The PCI Data Security Standard (DSS) is comprehensive and specific enough to be the foundation for (or at least a component of) a solid information security program of any organization irrespective of size. The DSS includes requirements for security management, policies, procedures, network architecture, software design and development and other critical protective measures. Due to the breadth of areas covered by its requirements, the DSS can help an organization consider and address most areas of information security. In short it can act as a springboard to security compliance in letter and spirit.

Conclusion

Organizations that perceive PCI compliance to be a valueless, one-time activity are not getting the true worth out of the program. This perception reflects an immature and dysfunctional security program. The key to effective PCI compliance and information security in general is in the long-term commitment to consistent and focused effort throughout the organization. When PCI compliance makes the transition from being a one-time activity to a long-term corporate commitment and culture, is when a security program matures and becomes effective. The PCI Data Security Standard can be the launch pad to making this significant transition.

Rich Corbridge is Technical Services Manager, Security Services for AppLabs, the world's largest software testing and quality management company.