

PCI v2.0: Is Your Organization Prepared to Meet the New Requirements?

In October of 2010, the PCI Security Standard Council (SSC) released a new version of the Payment Card Industry (PCI) Data Security Standard (DSS). Version 2.0 demonstrates the PCI SSC's continued commitment to advancing the adoption of the standard which now incorporates improved flexibility, alignment with changes in industry best practices and clarifications to the scoping and reporting requirements.

Each year, PCI DSS non-compliant companies are unnecessarily exposed to the risk of customer card account data being lost or stolen. Financial institutions, restaurants, retailers and universities continue to be a favorite target of identity thieves. When the University of Hawaii made the front page of the Honolulu Advertiser, we learned that the islands are not immune to their attacks. While Hawaii is not typically on the cutting edge of technology and compliance topics, even medium to large Hawaiian companies now find themselves necessarily immersed in the challenge of complying with PCI.

Achieving compliance is not a one-time event, but actually a combination of business processes and technology that requires ongoing monitoring and auditing to ensure full data protection and compliance with the standard. As we enter the fourth generation of PCI, if you haven't yet spent the time necessary to understand how this version impacts your business, now is the time.

In this interactive discussion, Jim Cowing, CEO of Digital Resources Group, a PCI SSC credentialed Qualified Security Assessor (QSA), will bring together his local experiences in helping Hawaii-based companies become PCI compliant and island perspectives to provide an in-depth overview of PCI DSS 2.0 changes, challenges and solutions.

Attendees will learn:

- Who must comply with PCI DSS 2.0 and by when?
- What are the key requirements of PCI DSS and the latest updates of version 2.0?
- What strategies can be used to deal with PCI DSS 2.0 compliance challenges?
- How can PCI DSS 2.0 be used as a springboard to strengthen a company's overall data security posture and/or your governance program?
- How can your company simplify the effort and minimize the cost of complying with PCI DSS 2.0?

Securing the Cloud: Virtualization Risks and Rewards

As the adoption of cloud computing and virtualization technologies continues to grow at accelerated rates, some companies have overlooked the importance of security in their rush to reap the rewards of lower costs, faster time to market and reduction in infrastructure that virtualization technologies deliver.

As a newer technology, virtual machines are often less understood than their physical counterparts, and as a result, simple security mistakes can unknowingly leave sensitive data vulnerable to attacks. If you have deployed or are considering moving services to the cloud, it is important to understand the security challenges virtualization technologies introduce and what security best practices are required to minimize security risks.

In this interactive session, Jim Cowing, CISSP, CITP, QSA will explore top security challenges for virtualized environments and virtualization security best practices. Learn how to protect virtualized environments based on your company's risk profile and how specific PCI requirements can be mapped to virtual environments.

Attendees will learn:

- What security implications companies should consider before moving to the cloud
- What key questions should be asked when interviewing cloud service providers
- Whether some businesses are better positioned for virtualized environment than others
- How much risk is being taken to outsource business processes to a cloud service provider
- How does virtualization impact compliance requirements, such as PCI DSS

SPEAKER BIO

James (Jim) Cowing, CEO, Digital Resources Group (DRG)

Jim Cowing leads DRG's Information Security Consulting Practice with over ten years of security consulting experience and twenty years of financial services industry experience. Well known in the islands, DRG is currently providing data security services for many Kama'aina companies. Mr. Cowing is a CISSP, PCI-QSA, CISM and CPA who has helped thousands of financial services, ecommerce, enterprise, government and health care companies understand and fulfill the often complex and stringent security compliance requirements of their respective industry.