PCI Compliance - Process & Procedure - Cyber Security - Remediation - Evaluate

Overview

Belinda Mobley is a **Cybersecurity Business Analyst** specializing in Cyber Security and PCI Compliance (Credit Card Processing) projects related to potential audits or security breaches.

Don't React, Re-Think

Your company's Strategic Planning and Remediation Strategies should include payment processing and security breach protocol that is designed to allow the Business to continue operations.

The challenge for many small companies is that once a compliance issue arises there is no time to get a plan together before the need demands action.

When the Network or IT Operations team recognizes an issue, their focus is to shut down the path of the breach. Therein lies the problem, these are network/operations professionals - not Business Stakeholders.

Recognizing there is a problem and stopping the breach are *not* the same skills as managing the remediation effort for Business Continuity.

http://www.belindamobley.com

Set Your Company Apart

It takes more than having the best product or service on the market to be successful. Customers also have to feel secure when making purchases. PCI Compliance can be a sales strategy to show you care.

Be Prepared

When facing a breach or audit there are very specific documentation and log files that must delivered to the forensic/audit team. These artifacts are the only way your company has to discover the source of the breach and prove culpability.

Therefore it is mandatory to have Policies and Procedures in place at all times for:

- A secure environment for all transactions;
- A plan for Forensic Assistance;
- The correct Log Files, Network Diagrams, and Infrastructure Diagrams up to date and available;
- Monitoring of Secure Environments;
- Accountability for Administrators;
- Security Awareness and Training;
- Repeal unsecure payment methods;
- A plan for Business Continuity.

Call to discuss your plan:
(404) 819-4518

Pro-action Now Leads To the ABILITY to React Later.

Security Scans and Network Penetration testing are already NIST recommendations, but they are PCI Compliance requirements.

Don't allow your network to become the single point of failure for your compliance efforts. You must execute Vulnerability Scanning and Penetration Testing Policies and Procedures today.

The key to keeping a business stable is in a Strategic Plan of action with Policies & Procedures and Contingencies.

Business is like a spinning gyroscope. Within that spinning is a calm center that keeps it from falling over. If there is a broken piece, such as a security breach, then it will fly apart. We are challenged to insure that the security strategy leaves no piece broken or vulnerable; No function undocumented; No relationship misunderstood.

Together we can keep the center strong, and immediately know where to look for an unstable part of the spinning wheel.

Let me explain how!