

SDDCO's Big Push to Mind Their Private Business

[The SDDCO Group, CPAs and consultants, audits their own data protection policy and trials a new campaign, SPAR: Survey-Protect-Alleviate-Report. It's a call to action to join the fight to safeguard sensitive data.]

Jan. 30, 2013

The SDDCO Group was confident that its staff knew how to handle private information responsibly. After all, in a 60 year accounting, tax, and compliance firm with a financial services specialty, SDDCO employees were accustomed to heeding the rules of the highest industry authorities, including the AICPA, IRS, SEC and FINRA.

Indeed, SDDCO's privacy standards for sensitive information were embedded in most documents. Employment contracts held confidentiality clauses. Service agreements defined terms of non-disclosure. A Notice of Privacy Statement got updated annually per AICPA's privacy principles. Their online Privacy & Security Policy was posted at sddco.com. And the firm handbook and BCP outlined staff security protocols.

Moreover, robust IT safeguards were being maintained. Besides daily backup on tape, SDDCO data is replicated to offsite storage via 128 bit encrypted VPN connection and is retrievable in a disaster recovery within 24 hours. And network protections include the McAfee VirusScan AntiSpyware Enterprise and WatchGuard Firebox X550e firewall with specific inbound and outbound port redirection policies.

But were SDDCO's protocols enough? Cyber threats were universally mounting; even the toughest IT infrastructures suffered security breaches. Still, in the welcomed absence of data calamities, how could actual compliance with policy and effectiveness be measured?

Since you can't find what you don't seek, SDDCO formed the Privacy Project to regularly assess company compliance, deepen understanding, and enhance data security in all areas of the business. "The Privacy Project," said Richard Sobel, Partner, "supports SDDCO's overall goal of providing superior services to our clients in a secure protected environment." His committee performed external research, internal reviews of office systems, updates to hardware spreadsheets, observations of workplace behaviors, conversations with SDDCO staff, IT, and management, and the drafting of educational materials.

After potential privacy gaps were IDed, a sticky campaign was created because if the new plan didn't stick, the staff might not stick with the new plan.

Their campaign was a call to action.

SPAR.....Join the fight to safeguard sensitive information

Survey.....where and how sensitive data is stored

Protect.....sensitive client and company data

Alleviate...buildup of all unnecessary data

Report.....any suspected breach ASAP

To support the SPAR campaign, new guidelines were prepared with no assumptions of prior knowledge. A glossary of terms was assembled. Personal identifiable information or PII was clarified. The document retention time-line was revisited. Strong passwords were made mandatory. And how-tos were issued for the gamut of data challenges, including lockbox shredding; purging machines; use of encrypted USBs; and how to respond to invasive breaches, such as spamming, phishing, infecting, and hacking. Next, the new content was placed in context with a data dilemma Q&A.

After all was said and read and done, SDDCO added another layer of security to their network server, the RSA SecurID, two-factor authentication system. Now access to the SDDCO network required staff to employ one-time passwords in addition to entering their own. Employees would use their smart phones to open personal software "tokens" generating new codes every 60 seconds.

Those one-off passwords and the SPAR campaign did command extra time, and staff grumblings were audible at first, however, the new systems soon became second nature. And while guarding data is an ongoing battle (current mission: laptop encryption), SDDCO is committed to minding their private business.

About SDDCO (<http://www.sddco.com>)

Born 1952 in NYC, The SDDCO Group delivers outsourced support to financial services clients including broker/dealers, investment advisers, privately held funds and the U.S. arms of foreign banks. SDDCO services include SEC and FINRA memberships, accounting, FinOp, tax, AML testing, brokerage advising and regulatory compliance. The continued success of the business is evidenced by a high rate of referrals and enduring client ties. For personal accounts of SDDCO service, see client testimony on the company site.