Don't Be a Box Checker

Bryan Miller, President
Syrinx Technologies LLC

Few topics in business management strike fear into the hearts of participants like *Compliance*. Compliance is often thought of in the same vein as death and taxes – something that is inevitable but if you ignore it long enough it almost goes away. Almost. In today's business world there are many challenges of compliance faced by management, including some of the more popular ones such as the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act (SOX), the Gramm-Leach-Bliley Act (GLBA) and the Payment Card Industry Data Security Standard (PCI DSS).

In case you find yourself under your desk cowering at the mere mention of these compliance acronyms, let me coax you back into your seat with a brief explanation. HIPAA was first passed in 1996 and attempts, among other things, to address the security and privacy of health data. There was an additional Privacy Rule enacted in 2003 which attempts to regulate the disclosure of private health data by various organizations. Sarbanes-Oxley was enacted in 2002, largely due to the public failures of companies such as Enron, Tyco International and WorldCom. SOX was created to require CFO's to take responsibility for financial reporting. GLBA was passed in 1999 to address privacy and data security for financial institutions. PCI was designed to protect credit card data and has undergone several upgrades over the past five years.

What do these compliance mandates have in common? They are all designed to protect consumers from abuses by those organizations that control access to sensitive data. Whether the data represents your personal health record, your financial statements or your latest credit card bill, the goal is the same. The guardians of that data have legal, ethical, moral and some would say religious obligations to protect that data. But you might ask, if everyone knows they have the obligation why so many regulations? This brings us to the concept of a "box checker."

Compliance is often seen as a necessary evil, something you have to do to stay in business like paying your taxes, purchasing insurance or paying rent. The business owners do not see their true obligation in protecting this data and therefore give lip service to complying with any applicable regulations. Their heart is not truly in complying because it's the right thing to do; they simply do as little as possible to pass inspection. The consequences of this mindset are seen too frequently in the media. It would take many pages to list all of the data breaches involving violations of the above regulations and many others.

So, a "box checker" is either an individual or a corporate mindset that says, "Let's do just the minimum so we can check the box on the next audit." What about your organization? Is it made up of "box checkers" or do you take seriously the responsibility for protecting the data entrusted to you by your employees and clients? If we all take personal responsibility we can reduce the aggravation and expense of cleaning up the mess left behind from a data breach. Think about your feelings when you had to replace your credit card. Ask anyone who has suffered identity theft about their thoughts on the subject. We all suffer from these events and it will take all of us to help prevent them.