The Security Trifecta

Breach Leads to Firm's Bankruptcy. This was the description of a Wall Street Journal article I read recently. What caught my eye is that it originated with a physical breach of the business location – yes, a kind of break-in. The intrusion resulted in the electronic exposure of roughly 14,000 personal records containing client addresses and social security numbers.

Now understand — this was not a super-slick hacking crime. This was an unsophisticated physical intrusion that led to the bankruptcy of a company. The reality is that with just a few simple, relatively inexpensive countermeasures, this would not be a business catastrophe.

First, data encryption would have prevented the exposure of those 14,000 customer records. There are solutions available ranging from the expensive to the free, so this is not a matter of technology being too expensive or exotic. This is cheap fundamental protection that has been available for a long time.

Second, access controls and monitoring for both the physical space and the electronic space is, again, commonly available for all budgets. The police have not caught the criminals and a simple web camera might have helped solve the crime**.**

The bottom line is this; security does not have to be complicated. It only takes the commitment to be more secure. I have spent my career within information security demystifying what for some is a like understanding a foreign language.

In my second book, Governance Documentation and Information Technology Security Policies Demystified, I introduce a concept I call *the Security Trifecta*. It is my security philosophy distilled into manageable facets. The fact of the matter is that by taking three well-defined pragmatic steps, we raise the bar and achieve success; governance documentation, technological enforcement and vigilant teamwork working together to promote security.

The Security Trifecta in brief:

- **Governance Documentation:** The foundation for what we do is based upon the written word. We collectively, collaboratively, cooperatively establish standards that are based upon philosophy, legal requirements, best practices, and regulatory demands.
- **Technological Enforcement:** When governance documentation has been established, we set about implementing and enforcing those standards as much as possible through the use of technology. Some technology implementations allow for the end user to exercise

greater choice and control, whereas others strictly enforce our standards taking the human choice element out of the mixture.

- **Vigilant Teamwork:** The reality is that nothing works very well without teamwork. Controls and standards breakdown without careful tending just like weeds take over our gardens without vigilance. We must regularly review our security standards, validating their relevancy. At the same time, we must remain agile enough to adapt to the changing business landscape, putting into practice carefully considered revisions to our ongoing security program.

The Security Trifecta is an effective and logical approach to information security I developed over the course of my career. The interesting thing is that the conceptual approach may also be applied to any other business process making it formidable to say the least.

As side commentary, the company I mentioned at the start of this tale is also facing the threat of even more debt as customers and individuals threaten to sue over the privacy breach. Unfortunately for victims, this may cost them much more than the expense of countermeasures invested up front.