Herding Cats:
The Cost of Ethics & Integrity

June 2009

BrandenWilliams
SECURE BUSINESS GROWTH

Ethics are expensive.

Think about that for just a moment. If you adhere to an ethical code, you will probably take more time to do your work, more pride in the output, and consumers will derive more value from your efforts. Your ethical code dictates how you conduct yourself while doing your work. You will ensure that you don't cut corners or cheat your customer. Therefore, in many cases, work done by someone who lives by a strong ethical code will be better than work done by someone who ignores ethics. Ethics cost more.

Most of us receive basic ethics training as part of our certifications. Thinking of the professional certifications I have earned over the years, I can't recall a respected certification that did not require all of its awardees to adhere to a code of ethics. If you choose not to follow the code of ethics and are caught, your certification will probably be revoked. That's one of the intangibles that comes with certification; respect and integrity is built in.

Integrity is another expensive trait. Our peers, managers, customers, and general acquaintances value integrity. It's a trait that must be demonstrated multiple times before it can be earned, but becomes one of your most prized assets when you do earn it. Integrity costs more.

So why do I keep referring to these traits as being expensive and costing more? Let's explore how it relates to compliance. Compliance affects everyone in our profession. Some of us have used it as justification for security spend, and others can't say the word without adding a violent stream of colorful metaphors in its close proximity.

Compliance initiatives (at least security-based ones) tend to be born as a solution to one particularly rampant problem. While the foundation of most security related compliance programs are rooted in established standards like ISO, they all have a tailored spin to uniquely address their environment or sandbox. In some cases compliance with a standard is simply a competitive advantage, while in other cases not complying could lead to substantial fines or negatively impact your business in some other way.

Have you ever heard the phrase, "You're compliant[1] until your caught/breached?" Merchants that accept credit cards must have had conversations like this in the past—especially those that thought they had an adequate security program. Imagine a company without a strong sense of ethics or integrity signing compliance attestation forms, knowing they had compliance gaps.

Could this explain part of the virtual crevasse that divides security and the business? I'm not suggesting that the business side does not have any ethics. What I am suggesting is that the folks on the business side are not aware of the ethics to which we certified professionals must uphold.

If you asked someone on the business side to commit fraud, we all hope they would say, "No way." They should have their own ethics and integrity to prevent them from taking this leap. Unfortunately, this is not always the case, and it does not affect only those on the business side of the house. We all know a security professional that either skirts the ethical line, or is so far over that line that you need megaphones to have a conversation.

FOOTNOTES

[1] I have heard this mostly in reference to PCI DSS, but believe it is even more true with HIPAA or GLBA. HIPAA is compliant driven, which emphasizes this concept.

For those seeking personal gain, they may weigh the risk of being caught with the reward of cash, and decide it is worth the risk.

That's Risk Management 101—something that all corporate managers claim to be.

Let's revisit compliance for a moment. If you require some kind of assessment or audit to achieve compliance, and it is required (or strongly suggested) as a part of your business, isn't it worth the extra money to ensure that you have found people with ethics and integrity to perform this assessment for you? The worst thing that can happen is that you find out that you are not compliant with a standard when you have been operating under the assumption that you are.

This concept is not only for your outside firm, but must be instilled in your executive management and pushed down to the individual contributors that are responsible for maintaining compliance. It's not the cheapest; especially with myopic monthly financial managers. It is the most responsible position to take, and will benefit key stakeholders as the threat landscape continues to change.

About the Author:

Branden R. Williams, CISSP, CISM, CPISA/M, has been making a name for himself in the Information Technology and Security arena since 1994, as a high school Junior. Now, a graduate of University of Texas, Arlington earning his BBA in 2000 with a concentration in Marketing and the University of Dallas, where he earned an MBA in Supply Chain Management & Market Logistics, in 2004, Williams is sought after as both an Adjunct Professor and Information Technology & Security Strategy Leader in the corporate world.

Williams regularly assists top global retailers, financial institutions, and multinationals with their information security initiatives. Read his blog at or reach him directly at http://www.brandenwilliams.com/.

TEL 214 727 8227
FAX 214 432 6174

BLOG brandenwilliams.com

EMAIL brw@brandenwilliams.com

brandenwilliams
SECURE BUSINESS GROWTH