Herding Cats:
Love the Lawyer You're With

May 2010

BrandenWilliams
SECURE BUSINESS GROWTH

Are you connected with your legal team? If your answer is anything other than "I go over my texting limit on my cell phone plan every month because I am so connected," then why the cuss not?

Lawyers have a bad stigma in our overly litigious society[1], though anyone who has had to retain one knows their value. After dealing with the minutiae of PCI DSS for many years, I know what it is like to take a somewhat rigid code and apply it to an imperfect world. I am in no way a lawyer or a student of law, therefore I cannot directly relate to what it is like sifting through millions of pages of precedent to find the right argument for your client. Regardless, the good ones are worth every penny when they are on your side.

And when you have an incident, you better have a good one on your side.

Some of my favorite discussions around information security and the law come from legislation recently enacted or interpreted on a state or federal level. Sure, PCI DSS by itself is pretty fun, but when Nevada[2] enacts a law that requires compliance to PCI DSS, things get pretty interesting. It only takes one moderately populous state enacting a law around industry compliance to start a nationwide snowball compliance effort[3].

One thing quickly becomes apparent when security professionals talk about the law—we are not lawyers. Oh the times I have heard a security professional use terms like "I think," "probably," and "should" when talking about legal issues that touch on information security. If for no other reason than that one, you should be sure you retain qualified expert counsel to help you navigate the new reality of using and maintaining information deemed sensitive by law.

Here are a few examples of places where your legal counsel should be helping you:

Data Retention Policies: While it may be the information security or IT departments that design or conduct operations under these policies, you should never enact one without having a lawyer review its contents. There may be strange things buried in state or federal legalese to consider when determining retention policies around certain types of data. For example, there may be some case law a lawyer is aware of that states certain data must be maintained indefinitely. In other cases, your lawyer may determine that other kinds of data should be maintained only for three years based on the legal risk and liability associated with keeping it.

Incident Response Procedures: If you have an incident, you will need lawyers at some point during the process. Get them involved up front and avoid the backlash you might get for unknowingly doing something to hurt your company's position should legal action be taken against it. They may require certain timelines for notification to certain parties, or depending on the data, they may want to engage either outside counsel or law enforcement more rapidly than you anticipate.

FOOTNOTES

[1] Overly litigious in the USA anyway. I understand that customs and laws in different regions of the globe may not see this problem. But when you consider that criminals have sued victims (and won) in the US, you understand my point.

[2] Nevada SB 227: http://bit.ly/abbvfw

[3] Depending on how it is written of course, but most are written protecting the residents of the state. Thus, even if you don't do business in Nevada, but a Nevada resident does business with you, you may have legal liability in the event of a breach.

Copyright 2010 Branden R. Williams. All rights reserved.

Insider Fraud: We all like to think we can trust our own employees, but not everyone is on the straight and narrow. As an extension to the above point, insider fraud may be treated completely differently than an external threat—especially if your company wants the option to press criminal charges or bring a civil case against the offender.

Sensitive Security Assessments: We all know every company has one or two skeletons in the closet. If you are doing a security assessment that might expose one of those to a larger audience, be sure your lawyers know about it first. You don't want to skirt your legal responsibility and duty to protect data, but you also don't want certain data about your company ending up in a legal discovery request by an attorney general.

If you don't have friendly legal counsel, it's time to take the plunge. If you already have counsel on staff or retainer, take the time to get to know your him and be sure he is well tuned into what you are doing.

Copyright 2010 Branden R. Williams. All rights reserved.

© 2010 Branden R. Williams. All rights reserved.

All material in this document is, unless otherwise stated, the property of Branden R. Williams. Copyright and other intellectual property laws protect these materials. Reproduction or retransmission of the materials, in whole or in part, in any manner, without the prior written consent of the copyright holder, is a violation of copyright law.

Contact information for requests for permission to reproduce or distribute materials available through this course are listed below.

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, buy his book, 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