



WHITE PAPER

Security Assessments and Investigations

– The Role of Lawyers and IT Professionals

Let's say you are worried about whether or not you're in compliance with some law or regulation concerning privacy or security. You have some reason to believe that you may not be in full compliance with; say the provisions of GLBA, or your contractual obligations under the PCI rules. You might be concerned about the status of your HIPAA compliance. Or you are considering rolling out a new product or service, and are worried that it might conflict with your obligations under the law. In these situations, it is typical for a company to conduct an assessment or evaluation, either conducted internally or externally. A company might hire an IT professional, an auditor, or some other third party to conduct the assessment, and generate a report on compliance together with a series of recommendations if it finds areas where compliance may be weak. Sounds like a good idea, and something that happens every day, right? In the words of Julie Roberts in "Pretty Woman," "big mistake... big." But why?

The problem lies not in the assessment itself, or even in the contents of the report. The problem is WHO is conducting the assessment and why. If the assessment is conducted for the CISO so he can understand the technological issues related to compliance, then, in the event of a later breach or lawsuit claiming negligence, the report not only becomes discoverable, but also becomes Plaintiff's Exhibit #1. If the report recommends that 20 things be done, and only 10 of them are actually implemented, then a jury could be persuaded that not doing the other 10 was negligent. Indeed, the perfectly reasonable assessment becomes a roadmap for litigation. On the other hand, if you DON'T conduct an appropriate assessment, you run the risk of also having liability for taking the "ostrich" approach to security. So what can you do?

Increasingly, companies seeking to become secure in order to both be compliant with regulations and to limit their risk and liability are turning to lawyers trained in IT security and privacy. These lawyers can not only advise the client about the requirements of the law, but can DIRECT and SUPERVISE the conduct of the evaluation. In this way, the results of the evaluation may be protected from discovery and disclosure at attorney-client privileged communications or attorney work product.

If a client – even a corporate client – is seeking legal advice or representation – such as "how do I comply with this law?" then the communications made to counsel or the agents of counsel to effectively obtain an opinion are generally protected from disclosure, as are the lawyer's response. It is important to distinguish between general business advice (how do I get secure) and LEGAL advice (what is my potential liability), with the law only protecting the latter. The law goes beyond protecting just the communications between counsel and

his or her client. It also protects the work that the attorney does – or has done on his or her behalf – in order to answer the question of the client. Thus, if IT security professionals work under the direction of and on behalf of counsel in conducting the assessment, the purpose of which is to provide effective legal advice, the work of the assessors is likely to be considered to be privileged or protected, at least at the outset. Courts would then have to consider whether the goal was truly legal advice, and whether there had ever been an effective “waiver” of the privileged. However, having competent counsel involved in the process can help get unbiased and open communication about potential risks and liabilities.

The same is true when a client suffers a data breach. Using counsel to conduct the investigation can help encourage more open communication by presumptively cloaking the entire investigation in attorney client privilege. While data breach disclosure laws likely will require disclosure of the FACT of a breach (if certain types of information are involved) issues like the source and impact of the breach can be evaluated and potentially protected from disclosure. If disclosure is ultimately made, this can be done on a reasoned and informed basis.

At SecureITExperts we have incorporated counsel into the process. Our lawyers have over 25 years experience in IT security, privacy and compliance law, and are trained and experienced investigators. Let us work for you.

