GOLDBERG & GOLDBERG, PLLC
Washington, D.C.
www.goldberglawdc.com

Rules of Engagement: Mitigating Risk in Information Security

TECHNOLOGY | CORPORATE February 13, 2017

Information security work, from pentesting to auditing, incident response to forensics, can be plagued with legal risks. A consulting job that covers one area may leave others vulnerable. And even total control may not prevent a later intrusion or breach, as the risk of "0 days" and failed vendor-supplied patches cannot be completely eliminated. Moreover, the work itself may be fraught with danger: servers knocked off-line, sensitive data in the hands of consultants-and subject to third-party subpoena, and even lawsuits by unknown third parties.

The solution is to set clear "rules of engagement": what to do about sensitive data; how to handle subpoenas and search warrants; and the scope of liability limitations and indemnification. The following six provisions are essential in any set of rules of engagement.

1. Explicitly state what will be done and what will not. For instance, an agreement should explicitly note whether a company is conducting an audit but not a pentest; or if there will be pentesting but only on test systems, not production systems; or if certain systems will be off limits to incident response.

2. Establish how sensitive information should be treated. In addition to the standard boilerplate about confidential information, it should state what a company must do in the event it receives a subpoena, national security letter, or civil investigative demand. This requires more thought than simply requiring that the company acquire a protective order—as many corporate lawyers do not understand that judges do not simply give out protective orders like candy; some may not be obtainable.

3. Clearly delineate access to systems or networks. If incident responders or pentesters should only have access to certain systems and not others, this must be made clear-in writing. This not only ensures that security professionals will not improperly access sensitive systems accidentally, it will also provide evidence of limited access in the event that the client later claims those systems should have been addressed. Furthermore, in the event there is a failure, the reporting structure must be agreed to, in advance.

> The solution is to set clear "rules of engagement" for security services, to deal with sensitive information, subpoenas, and liability limitations.

4. Agree to the bounds of phishing e-mails and other social engineering. For instance, high-quality phishing may include the use of logos and trade names to which the security professional may not have rights. The legality and liability for such work must be clearly assessed and the risks weighed.

5. Set forth limitations of liability. This means establishing ceilings on money damages and may even include negligence. It may also include indemnification against third-party suits, especially in which victims of a data breach sue the company's auditor. The first such suit was in 2009, against a

PCI auditor. It was settled on undisclosed terms. More recently, following a data breach at a major retailer, the security auditor was sued for negligent auditing. It was later dropped from the suit, but at the time of this writing, the option to re-file remained.

6. Acquire insurance. Regular errors and omissions insurance may not cover even run-of-the-mill security work, which may require so-called "cyber policies" and other industry-specific policies. One must keep in mind that insurance may not cover so-called "contracted-for" risks, in which the insured agrees to additional liability voluntarily, through contract. It also may not fully cover defense costs; or, more commonly, it will require the use of attorneys selected by the insurance company itself.

These items, in addition to the typical provisions concerning payment, notice, and standards of care, make up the basics of any agreement for security services. Others may be required for specific kinds of work.

The most important thing to recognize is that information-security contracts are not like other technology contracts for services or software. In many cases, the stakes are far higher, because so much can go wrong. And that means agreements must be more-carefully drawn and rules of engagement agreed to in advance.

If you would like to discuss how these issues could affect your business, or if you would like to discuss other contracting issues, contact Richard Goldberg.

Attorney Advertising: This material has been prepared for general informational purposes only and is not intended as legal advice.

GOLDBERG & GOLDBERG, PLLC
1250 Connecticut Avenue NW, Suite 200
Washington, D.C. 20036
(202) 656-5773
www.goldberglawdc.com