Rendigs
ATTORNEYS AT LAW

Business Briefs
Legal Update

Donald C. Adams
Partner

Email: DCA@Rendigs.com
Direct: 513 381 9361
Fax: 513 381 9206

The Legal Repercussions of a Cyber Security Breach Part 2/3

This article is the second installment of a 3-part series on cyber security.
Read Part 1 here.

When a computer security breach occurs how should it be handled with customers and clients? Is there immediate public disclosure, or is there first a careful investigation and scrutiny of what occurred and what data was compromised? The proper strategy must be developed preemptively along with related training to instruct employees how to handle the issue. The most forward thinking businesses go a step further and conduct training simulations with employees to simulate cyber attacks and data security breaches.

Can I be sued if I'm hacked? Aren't I the victim?

When cyber attacks happen, clients, vendors or others may take legal action. Claims of negligence, the breach of the standard of care, may be alleged by plaintiffs who have suffered damages resulting from breaches of computer security. Such plaintiffs can look to the vendors who designed the system including firewalls, encryption, and coding software. In addition, plaintiffs may allege the "hacked" system owners who failed to implement reasonable security measures enabled the hackers to obtain confidential information or use company systems to launch attacks against third parties or to spread viruses.

Currently there is no legislation and little case law defining the standard of care companies should take regarding cyber security. Further, like the internet, practices and methodologies are changing rapidly. Security procedures are being continually improved giving rise to a

Rendigs, Fry, Kiely & Dennis, LLP
600 Vine Street, Suite 2650
Cincinnati, Ohio 45202

moving standard relative to the risk exposure which makes maintaining a standard definition of care especially difficult.

The limited case law addressing the standard of care has looked to standards prescribed by the FTC in various matters giving rise to consent orders. These consent orders required the system owners to establish and maintain a comprehensive written information security program that is reasonably designed to protect security, confidentiality and integrity of personal information collected from or about consumers. The information security program must contain administrative, technical, and physical safeguards appropriate to the company's size and complexity, and the nature and scope of its activities.

So what's a business owner to do?

Today's emphasis on cyber security has resulted in the availability of substantial amounts of information relevant to the management of cyber security risks. Given the availability of such information, companies that fail to take basic steps to reduce cyber security risks and maintain a comprehensive program based on their level of risk are going to find it difficult to justify any failure to implement and maintain appropriate controls and defenses to avoid, reduce and mitigate damages. Basic steps would include updating firewall rules and hardening security, reviewing logs, and educating users to recognize and deal with malware, phishing, spear phishing and other suspicious emails, fake hyperlinks, and attachments.

On the other hand, a company that implements safeguards has to live by those self-imposed guidelines. If the cyber security policy is not adequate in the first instance a claim of negligence will be fairly easy to prove. Option 1: If the cyber security is designed in-house it needs to follow and comply with acceptable industry guidelines. Option 2: If an outside vendor is utilized there is some potential insulation from fault due to justifiable reliance on the expertise of the vendor in designing the security adopted. However if the vendor is not reliable or does not have sufficient resources or insurance to support a claim of indemnity, the company is still greatly at risk. Further, many vendor contracts have contractual clauses limiting liability or damages to actual repair of the system and excluding damages to third parties. It is best to have your attorney review these contracts and advise you on the risk your business is assuming.

A business owner must take steps to protect customer information. A minor security breach can give rise to significant costs, civil liability exposure and a loss of customer confidence. Perhaps the latter is the most significant because monetary recovery cannot repair customer loyalty. It is worthwhile to consult with legal and cyber experts to protect your future.

Don Adams'*s practice focuses on civil litigation in the area of medical defense litigation, transportation, maritime and wrongful death and injury. He defends hospitals, corporations, nursing homes, and physicians. He counsels clients on risk management and quality assurance matters.*