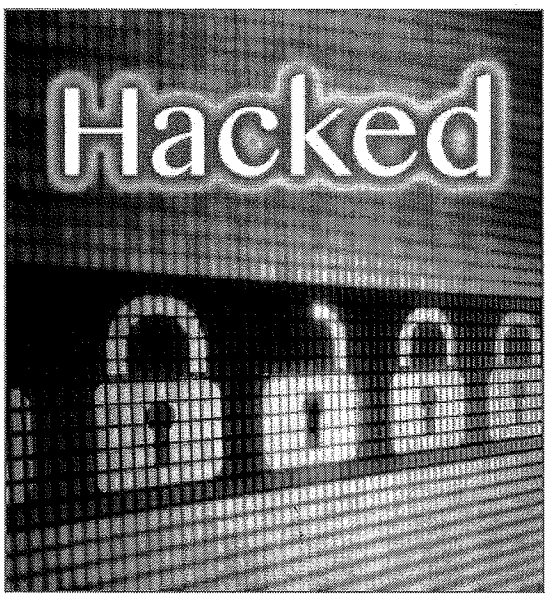
Virginia Lawyers Weekly **http://valawyersweekly.com**

Hacked: What to do if your office computers are breached

by Correy E. Stephenson

Published: May 20th, 2013



While stories of foreign hackers and data breaches may seem unlikely in the commonwealth, "it can happen to anyone," warned John Simek, vice president of Sensei Enterprises, a digital forensics and information security company in Fairfax.

Take the example of criminal defense firm Puckett & Faraj in Alexandria. Last year, the firm was one of several targets of the hacker group known as Anonymous. The firm had defended a U.S. Marine staff sergeant in a case involving the death of civilians in Iraq, which resulted in a conviction on reduced charges. Apparently protesting the less severe penalties for the Marine, Anonymous replaced the firm's homepage with a video of hip-hop artist KRS-One rapping about police brutality and posted the firm's emails on YouTube and other sites.

Neither the size of the firm nor the sophistication of the client base matters, Simek said. Family law attorneys have detailed information about clients' assets while personal injury attorneys may have treasure troves of data, including Social Security numbers and credit card information. And law firms representing corporations may be an easier target than the company itself for data-seeking hackers.

Although the Federal Bureau of Investigation has issued multiple warnings to law firms over the last few years that they are the targets of such attacks, practitioners continue to be lackadaisical about data security at a high cost to themselves and to their clients.

"Lawyers keep saying, 'That will never happen here,' but there is example after example of firms that have been breached," Simek said.

So what should law firms do if they get hacked?

First, stop the breach, said Roanoke lawyer W. David Paxton. Identify the access point(s) the hackers are using and the security weaknesses. If possible, preserve any relevant data to help track the hackers and determine what information was accessed – just certain client files? The entire system?

Second, investigate the nature and the extent of the breach, Paxton said, like the length of access and what information was involved in the breach, notifying the proper law enforcement authorities.

The next steps are the most complicated – and costly – for attorneys: notifying those affected by the breach and attempting to stop it from happening again.

State law, federal law, ethical obligations

In Virginia, lawyers face a multi-faceted series of obligations should a data breach occur, beginning with a state data breach notification statute.

Virginia Code § 18.2-186.6 applies to both public and private entities and kicks in when an individual's name in combination with one of three other pieces of information is unlawfully accessed – more than five digits of a Social Security number, more than the last four digits of a driver's license number or state identification card number or more than the last four digits of a financial account number, credit card number or debit card number.

Virginia also has a second data breach notification law relating specifically to medical information but it only applies to governmental entities or agencies supported principally by public funds.

The statute says notice must be given to affected individuals if the information "was or is reasonably believed to have been accessed and acquired by an unauthorized person and causes, or the individual or entity reasonably believes has caused or will cause, identity theft or another fraud to any resident of the Commonwealth."

Notice must also be provided to the attorney general's office and in cases where more than 1,000 residents are affected, to the three major consumer credit reporting agencies.

Notice must be provided "without reasonably delay" and should inform the recipient about the circumstances of the data breach, the type of information compromised and what the law firm has done to protect against a future breach, as well as provide a telephone number for additional information and assistance.

Affected individuals should also be advised to monitor their credit reports and account statements for unauthorized activity.

Encryption provides a safe harbor under Virginia law, Simek noted, so lawyers would be well-served to take advantage of such a simple solution. "Encryption is going to be your friend," he said.

Lawyers should also determine whether out-of-state residents were impacted by the breach. While Virginia's data breach notification law is similar to those found in 45 other states, different requirements may need to be met for non-Virginia affected individuals, Paxton noted.

In addition to Virginia's data breach notification law, some law firms may also be covered by the federal Health Insurance Portability and Accountability Act (HIPAA) and its 2009 counterpart, the Health Information Technology for Economic and Clinical Health Act (HITECH), said Richmond attorney Jonathan M. Joseph.

Practitioners who maintain health information must comply with security and privacy rules found in the federal laws, which includes breach notification requirements.

Separate from other businesses, lawyers face additional obligations to notify their clients in the event of a data breach, said McLean lawyer Thomas E. Spahn, who advises companies on ethics and professional responsibility.

Pursuant to Rule 1.4(a) of the Professional Rules of Responsibility, Spahn said lawyers have an ethical duty to inform clients about a data breach if client confidences may have been disclosed – a requirement above and beyond the data breach law itself.
In addition, if malpractice may be a concern, lawyers have yet another notice requirement, Spahn added.

A parallel obligation to a lawyer's ethical duty, a potential malpractice claim would be based on the standard of care provided to a client. So if a highly skilled hacker located in China accessed a law firm's website, malpractice might be less of an issue. But if a lawyer left a drive containing a back-up of the firm's entire system on the train and it was stolen, the question of malpractice could arise.

"The Virginia bar has said that lawyers have a duty to tell a client if the lawyer has committed malpractice," Spahn said. If there is any chance that the breach was due to malpractice then the lawyer would again be responsible for informing the client – and face a potential malpractice suit.

Reduce the risk

To minimize the chances of a data breach – or avoid a subsequent malpractice claim – law firms should proactively consider their data security.

"Identify a data breach prevention and response team to conduct internal audits and develop and periodically review company policies and security," Paxton suggested.

Simek recommended that firms conduct an annual "vulnerability assessment" to review their system, policies, processes and procedures. The review allows a firm to get a professional opinion about their data security needs and prioritize what needs to be done to improve security.

In addition to some simple tips to increase data security (see below), Simek suggested that law firms

explore the option of cyberinsurance.

A data breach and the resulting costs will not be covered by most general liability insurance. Lawyers could end up paying out of pocket for the cost of notification, the possibility of identity theft protection and credit reporting for affected clients and any ensuing repairs or upgrades to their system.

"It's cheaper to beef up security on the front end," Simek said.

---

5 simple tips for better data security

Imagine getting up in front of your peers to make a presentation. The next thing you know, pornography pops up on the screen. Sound impossible? It happened to a colleague, John Simek said, but it could have been prevented with a simple security tip: screen locks.

An investigation revealed that a member of the cleaning crew at the colleague's office enjoyed surfing adult websites and was able to do so because the computers that were left on did not require a password for access nor did they time out after a period of inactivity.

"This is an egregious example," acknowledged Simek. "But it can happen if your system is not secure."

And the embarrassing twist to the presentation could have easily been prevented with the addition of an inactivity timer requiring a password to log back onto the system – Simek recommends setting the timers between five and 10 minutes.

Below, Simek offers five other quick and inexpensive security tips.

Physical security. "I should not be able to walk down the hall at a law firm and open doors to reveal servers or routers," Simek said. Put a lock on doors and cabinets that contain important technology and limit access to just a few employees.

Secure the network. Offering free wi-fi in the office may seem like a client-friendly move, but it only heightens the security risks and invites unwanted guests onto the system. Add a password, Simek said, and change it frequently.

Password strength. Law firms should require system users to change their passwords on a 30-45 day cycle, Simek recommended. "It's a simple thing to do and yes, it's a pain, but that little thing is going to go a long way towards improving security."

Change the defaults. Never, ever use the defaults provided with software or hardware. Whether default user ID or password, change it immediately. "The defaults are well known," Simek explained, and a Google search can reveal what the defaults are for a given product – making access that much easier for a hacker.

Patch and stay current. Staying on top of security patches and updates may get pushed to the bottom of the priority list but being out-of-date can also be a security risk. "There is a reason why they release this stuff," Simek noted. Remember to remain current not just with systems like Windows but also for any apps, he added.

Complete URL: **http://valawyersweekly.com/2013/05/20/hacked-what-to-do-if-your-office-computers-are-breached/**