GPSOLO eReport
Vital Information for Successful Practitioners

## Four Easy Ways to Prevent Data Breach at Your Firm



### Four Easy Ways to Prevent Data Breach at Your Firm

Vol. 1, No. 11

David Gracey

*David Gracey is a graduate of the Georgia Institute of Technology, where he earned his bachelor's in industrial engineering in 1989. He started Network 1 Consulting, an IT support company in Atlanta, GA, in 1998. Network 1 can be found online at www.network1consulting.com.*



- Learn how hackers discover your computer's vulnerability.
- Find out what kind of firewall you should have.
- Learn how to make an easy password difficult to crack.



Every week brings national news of yet another corporate security breach costing a company hundreds of thousands of dollars in damages and fines. With the vast resources spent on protecting the IT infrastructure of Fortune 500 companies, how is the small law firm supposed to protect itself on a limited budget? The answer is much simpler than you would think. Let's start with the bad news first.

Just like a burglar who targets a home for a heist, if a bad guy targets your firm's computer network for electronic penetration, *and has enough resources*, there is not a whole lot that can be done to prevent him from gaining access to your system. This leads to the good news: it is extremely rare for a small firm to be the target of a highly focused attack. The reason is that law firms and small businesses almost never have enough valuable information stored on their servers to become a target in the first place. If you are a cybercriminal, it is much more interesting to steal Facebook's password database or Chase Banks' credit card list than your briefs, contracts, wills, and articles of incorporation.

Now that we have accepted the fact that it is possible for bad

### About GPSolo eReport

*GPSolo eReport* is a monthly electronic newsletter of the ABA

guys to access our systems, let's figure out what to do to protect against the real threat that exists: the casual hacker. Hackers come in three main types:

- Recreational hackers: these are guys (they are almost all males) who, if born in a prior generation, would have spray painted a bridge or vandalized a building. Today, a kid (they are mostly under the age of 25) armed with average computer skills and Google, can access millions of vulnerable systems. Most are looking for recognition among the hacker community or simply enjoy the sport of it. Like destroying physical property, many hackers enjoy deleting data or rendering computers inoperable. Needless to say, the casual hacker can cause your firm real damage.
- Hacker for hire: these individuals and small groups are hired by others who are trying to get databases such as credit card numbers, Social Security numbers, names, or email addresses, which can be resold to others on the black market. Your name, address, and credit card number is worth about $8 on the black market.
- Espionage: the CIA is very active in electronic surveillance and has about as many resources as they need to pull off some amazing feats, most of which go undetected for years. If you're the target of one of their attacks (in the United States there are laws against that), you won't know what hit you until they are done with you. Both Iran's nuclear program (Google "Stuxnet" for more info) and thousands of computers in the Middle East (Flame virus) have been on the receiving end of these attacks. What these attacks do is nothing short of amazing.

So unless you are assisting Al Qaeda or storing a lot of credit card information, the most common threat you will face comes from the recreational hacker. Fortunately, there are several simple and inexpensive steps that can be followed to greatly reduce your chances of being hacked. I'll share those steps below. But first, a little more background on the recreational hacker.

With the recreational hacker, it's a numbers game. There might only be a small number of vulnerable computers in your office, but if the hackers scan thousands of them, they will get a large number of targets, possibly including yours. This is how a hacker finds you: first, the hacker downloads a free software tool that is designed to scan vast numbers of computers. He can target a geographical area like Atlanta, but most times he will just set it to scan all the computers in a given region, which will generate tens of thousands of hits. After a day or so of scanning, the tool generates a report that shows all computers that fit his criteria—say, all computers that have Microsoft Windows installed. His next step is to get another tool that will "knock on the door" to see what electronic ports are unprotected. Over the years, hundreds of bugs have been discovered in Microsoft Windows, and patches have been released to fix most of them. The problem is most people don't update their Windows software very often (if ever), and the hacker's software tools know how to exploit those bugs, thereby gaining entry to your system. Once the hacker has his list of vulnerable computers, he can then manually take control of the remote computer and install other tools that allow

General Pratice, Solo and Small Firm Division that combines elements of *Solo, The Buzz, GPSolo Technology eReport,* and *GPSolo Law Trends & News*. Its purpose is to to put clear, comprehensive, cohesive, useful, and timely information into the hands of Division members.

- Visit the ABA General Practice, Solo and Small Firm Division
- More publications from the General Practice, Solo and Small Firm Division

## Subscriptions

A subscription to *GPSolo eReport* is included with your $45 annual dues payment to the General Practice, Solo and Small Firm Division. You can join the Division by visiting the ABA membership website or calling the at 800-285-2221.

## More Information

- Copyright information
- Advertise with us
- GPSolo eReport Editorial Board Members

## Contact Us

Thomas Campbell, Managing Editor
American Bar Association
321 N. Clark St.
Chicago, IL 60654-7598
Phone: 312-988-5990
Fax: 312-988-6135

Kimberly Anderson, Director

him full control of the system. At this point he can do whatever he wants to the computer, such as storing other files there, copying off or deleting all the data, or doing other mischief. Once a computer system has been breached, the only guaranteed way to ensure the computer is secure again is to wipe out all the information and reload everything from scratch.

If a computer on your firm's network is compromised, the hacker then has the ability to begin taking control over other computers and servers on your network. The best plan is to be proactive and keep the hacker from breaching your security perimeter in the first place. There is no single security solution to protect everything. Instead, security is best managed using a multilayered approach. You need several different protocols in place in order to minimize your risk of a security breach. Fortunately, the four most effective ways to secure your network are easy and inexpensive to implement.

## Install Software Patches

The most common way in which a hacker accesses a computer system is to exploit well-known bugs in the Windows operating system. Again, it's just a numbers game. More than 90 percent of all computers in the world run Windows, so hackers have a big pool to draw from. To make matters worse (or better if you're a hacker), many computers run pirated copies of Windows, which cannot be updated.

## Robust Firewall

A dedicated hardware firewall is your best defense against the public Internet. Firewalls come in many types and price points. Although the $100 special that can be purchased from your local Best Buy or Office Depot can keep out a good many of the bad guys, what the job really calls for is a robust, business-class firewall that has advanced intrusion prevention, built-in antimalware capabilities, and detailed reporting. Additionally, it should be monitored by an IT expert who knows what to look for if a data breach is being attempted.

## Antivirus Software

Good antivirus software has been around for years, but as the threats have evolved, so has the antivirus software. Antivirus, which also includes antispyware and antispam, is now known as antimalware or end-point protection. But regardless of the name, pick a market leading provider such as McAfee, Trend Micro, Norton, or Kaspersky. Make sure it's installed properly and monitored by your IT expert to ensure the definitions are updated

American Bar Association
General Practice, Solo and Small Firm Division

Jeffrey M. Allen, Editor-in-Chief
Graves & Allen
Oakland, California

at least daily.

### (Not So) Complex Passwords

A hacked database last year revealed passwords for millions of online accounts (see RockYou.com). Of the top 10 most commonly used passwords, 12345 (number two on the list) or 123456 (number one on the list) or similar strings make up five of them. "Password" is the number four most commonly used password. Having a strong password for all computer accounts is one of the toughest to implement. There is always someone, usually a partner or owner, who wants to keep his password as 1234 or worse, blank. Because security is only as good as its weakest link, this habit must change. Hackers use "dictionary" attacks to continue trying common words in our vocabulary, so computer owners need to make it tougher for them. I'm not asking folks to use a long, highly complex password of mixed numbers and symbols, but rather take a word you know, preferably at least 8 characters long, and just replace a letter with a number and add a capital letter. So for instance, a simple password like "lawfirm" can be made much harder to crack if it is changed to "Lawf1rm".

Being the victim of a data breach is bad for your firm, your clients, and your reputation. Putting in place a few simple steps can greatly reduce your risk of a data breach. More importantly, having someone at your firm asking your IT expert the tough questions and holding him accountable is a critical part of keeping your system secure.