ASK THE EXPERTS

Help: How Can We Guard Against Cyber-Attacks?

By The Editors | Feb.18.13 | Ask the Experts, Daily Dispatch, Management, Technology

Question: Cyber-attacks are on the rise, and our firm is very concerned that client confidentiality may be compromised. What are some of the short-term and long-term tactics we can implement to minimize this risk?

ALA Association of Legal Administrators
ASK THE EXPERTS
From the Association of Legal Administrators

Robert Baumgarten: "Unwilling Zombie Pawns of the Ne'er-Do-Wells." The battlefield upon which we engage cyber intruders has shifted from the server rooms and data centers to the space occupied between the desktop and the chair—to the attorneys, paralegals and administrative assistants. Law firm IT professionals already understand what weapons are available to prevent the onslaught of cyber intrusions—from the basics of patching and application whitelisting to dozens of more sophisticated mitigation strategies. Ask and they will tell what they need, as well as the cost and the benefit of action or the danger of inaction. They'll also confess the cold, dark reality that no firm, client, corporation or country is impervious to attack.

We must utilize some of the same strategies employed by our adversaries if we are to persevere. Initiate a persistent, targeted and ever-evolving campaign of end-user awareness—a steady drip, drip, drip of security-minded information, ranging from emerging threats to developing scams, to constant reminders of the dos and don'ts, and real-world examples of things that go bump in the night—so that when they see something, your end-users will say something because they recognize the threat for what it is. By constantly feeding your users bite-sized pieces of awareness, eventually you create a formidable army that is part of the solution—and not the unwilling zombie pawns of the ne'er-do-wells.

Robert J. Baumgarten is the CIO at Shulman, Rogers, Gandal, Pordy & Ecker in Potomac, MD, and has more than 20 years of experience in cyber-security issues facing law firms. He is the father of four, a former Marine, and an avid sailor.

Elias Montoya: "The biggest threat is your own internal users." With more firms vying to go paperless, more client data resides on our computer networks. Along with the great benefits of digitizing client documents comes the increased risk of unauthorized access to that data. IT network policies that align with sound risk management should be the basis of network security practices. However, even the toughest measures meant to keep intruders out are not good enough.

The biggest immediate threat is your own internal users. Their lack of knowledge, combined with the ingenuity of hackers, makes them the primary target of cyber-crimes. Investing time and resources in educating attorneys and support staff, in conjunction with sound policies, is the best way to minimize such risks. Educate people on the importance of security, why policy exists and the consequences of not abiding by such policies. They should know the ultimate goal of these policies is to protect the firm and the client's data, which everyone has an obligation to protect.

Social networks are big threats to system security. Just like emails before them, hackers and cyber-criminals are now exploiting the social networks, and law firms should be taking note. Malicious links abound on the social media sites, and user accounts are hacked regularly.

The use of smartphones with third-party email access, along with seamless integration with social media—such as Facebook integration with the contacts management apps on smartphones and tablets—presents risk. Imagine someone from your firm writing a confidential email and mistakenly sending it to the wrong person, or worse, to a social network. When that happens, that information is integrated into the social media servers, where it should never reside. Even worse, it can be posted, exposing information publicly.

In this evolving "bring your own device" era, policies and control measures should be reviewed to minimize a data breach.

Elias Montoya is Technology Director at the Miami-based Abadin Cook, where he oversees and manages the firm's IT operations as well as litigation support services. He was the main architect of the firm's paperless workflow system, making Abadin Cook one of the first paperless law firms in South Florida.

John Sroka: "It's no secret, since late 2009 the FBI has been warning law firms about noticeable increases in cyber-attacks." Hackers consider law firms soft targets with a high concentration of critical, private information. This was reinforced again in January at LegalTech New York by an FBI security expert. Firms' needs and security requirements will vary. However, there are basic defenses that should be employed by all.

- Use strong passwords. Passwords should be more than six characters, using a mix of case letters, numbers and symbols. Passwords should also be required on all mobile devices and changed regularly.
- Install firewalls and keep rules updated.
- Develop and enforce Internet and technology usage policies.
- Provide security awareness training.
- Keep your computer, browser antivirus and other critical software up to date.
- Do not open an email or attachment from an untrusted source.
- Pay attention to website URLs. Malicious websites may look identical to a legitimate one but the URL may use a variation in spelling or a different domain. Do not click on unknown links.
- Monitor security logs.
- Restrict access to sensitive data.
- Password-protect laptops and encrypt hard drives.
- Do not write down passwords.
- Do not install software from unknown sources or unknown websites.
- Do not use Dropbox or other Internet file-hosting services for client documents.
- Media such as USB drives should be encrypted.
- Servers should be in a locked room.
- Do not share your user ID or password.
- Use a screensaver password and always log out when away from your computer for a period of time.

John J. Sroka is CIO at Duane, Morris LLP, overseeing all aspects of technology-related initiatives, including practice support, Web development, help desk, training, telecommunications and network services. In 2007, John was named "IT Director of the Year" by Law Technology News' 5th Annual Law Technology News Awards.

George Theochares: "When '60 Minutes' is knocking on your door, it's too late." Recently Secretary of Defense Leon Panetta warned in a speech at Georgetown University that "a hostile country could attack America by computer: a 21st century Pearl Harbor." Cyber security is no joke, so make it a priority and use a commonsense approach to prevention.

- Create and enforce clear and concise policy. Massachusetts' data protection law MA 201 CMR 17.00 covers this with the WISP (Written Information Security Program).
- Audit regularly for compliance and have a backup plan.
- Secure handheld devices, social media sites you own, and telecommunication systems.
- You don't need to reinvent the wheel. Most technology vendors have contingency plans, so ask them for "best practices" and follow their advice.
- Don't fall into that minefield of one rule for me and another for everyone else.
- If you are breached, have a plan for that, too. Does your current insurance protect against hackers, viruses, data theft and IPR lawsuits? Does it provide tech insurance that safeguards your company's equipment, employees, intellectual property rights and reputation? Consider purchasing some.
- As always, have a backup-plus-continuity plan, and test. If there are glitches, fix them right away.

Will there be hoops to jump through? Will they make it harder to access data? Well, yes. It's a trade-off and a business decision. The bottom line: If it's important to you, it's likely important to someone else. Protect your interests.

George Theochares is the IT Director for Campbell Campbell Edwards and Conroy, with more than 17 years of experience in the legal profession and another 25-plus years in information technology and security.

Stephen Wilder: "Four Key Areas of Risk from Cyber-Attacks." When addressing risk it is often easiest to think of it in terms of four categories: (1) Avoidance, (2) Mitigation, (3) Management and (4) Transfer. With respect to cyber-attacks, risk avoidance is basically an impossibility. Therefore, firms need to focus on the other three areas:

1. **Risk mitigation.** This involves things like making sure the firm uses appropriate hardware and software to protect the firm's network and also keeps it up to date. If you use outside service providers, it is important to understand the systems and procedures employed by each provider. Further, the firm should establish a plan with the service provider for regular maintenance and updates to software and hardware. Finally, before selecting or switching service providers, the firm should ensure that the provider has the expertise and experience to address a law firm's particular needs, and make sure the provider is adequately insured.
2. **Risk management.** This comes establishing operational controls for the users of the firm's network—for instance, making sure users know not to open email attachments from unidentified sources. Although spam filters and security programs can catch most suspicious email, they are not 100 percent reliable, leaving the users as the last line of defense. The firm should also establish a policy for web browsing, but of even greater concern are "sharing" programs. Music-sharing programs, for example, often require you to provide access to your systems, or at least default to open access. This means that you are creating an open highway to the firm's network, bypassing established security measures. Finally, controls for laptops and off-site computers are very important. If employees store confidential information on a laptop or a portable memory device and take it off-site, they need to be aware that loss or theft of the laptop should be presumed a breach of confidential information. More often than not, this is where problems arise.
3. **Risk transfer.** Risk transfer occurs to some degree when a firm uses an outside service provider. However, this does not protect the firm from liability to its clients. It simply provides a potential avenue to seek reimbursement for the liability. Pure transfer is achieved by purchasing insurance addressing the various risks and exposures of cyber-attacks. Some professional liability policies provide limited cyber liability coverage that allows the firm to transfer some exposure, but not all. The best way to transfer the risk is to purchase a separate cyber liability/privacy policy that provides third-party exposure (attacks from outside the firm), first-party exposure (loss of data by employees or representatives of the firm), and crisis management coverage. Cyber liability is a relatively new product, so policies can differ substantially in the breadth and type of coverage provided.

Stephen G. Wilder is the Manager, Professional Liability Division, at M.G. Welbel & Associates, Inc., in Northbrook, IL. He is presenting on "Cyber-Attacks: The Liability Risks to Your Firm" at the 2013 ALA Annual Conference on April 16 in National Harbor, MD.

Rob Wilson: "You have an ethical responsibility to keep confidential information confidential." With the increasing sophistication of cyber-attacks, law firms need to make sure the proper technologies are in place to circumvent security breaches. Some guidance:

- **Knowledge is power.** Train both lawyers and support staff to report possible suspicious activity—for example, computer malfunctioning after accessing a website, unknown emails or communications, and requests for confidential information.
- **The power of the policy.** Put policies in place that outline the possible events in a breach and how to resolve them.
- **Patching power.** Make sure systems are up-to-date with the latest security service patches.
- **First lines of defense.** Make sure you have a firewall that will keep out potential threats to your network. Protect your systems with industry-standard virus protection. Set it to update *every hour*.
- **Passwords.** Set them to expire every so often and prevent users from using the same ones.

Awareness is the first step in protecting your firm from outside attacks and keeping your clients information safe and confidential.

Robin (Rob) Wilson is an Information Technology Manager at Wolcott Rivers Gates. He has more than 15 Years of experience with the installation, maintenance and administration of Novell and Microsoft networks.

Questions for Management?

No, not every law firm has a full-time administrator or professional management to guide them. Send us your questions via email, or use the comment section below, and we'll pass them on to the experts at the Association of Legal Administrators. Watch for the best ones here in "Ask the Experts."

ALA Association of Legal Administrators

The Association of Legal Administrators—Your Connection to Knowledge, Resources and Networking.