10
20
0
50
30

BY LARRY PORT

proper protection

Assessing your firm's data security policies and practices and making appropriate changes will ensure your firm's short- and long-term stability.

Paranoia is your friend. That's as good a mantra as I've heard for securing sensitive information.

Since networks began, law firms and other organizations have had to worry about all kinds of hackers, attackers and unsavory digital cretins. Then recently, the Cornficker worm reared its ugly head, infecting 30 perfect of all computers using the Microsoft windows operating system. Later, IT professionals had to deal with the repercussions of the Microsoft/T-Mobile Sidekick fiasco. And just when you thought it couldn't get any worse, hordes of Chinese cyberwarriors launched an onslaught against Gmail, Google's popular e-mail service.

This article strives to create a broad view and practical starting point for your firm to assess its data security policies and practices. To facilitate writing it, I contacted several IT professionals who are also members of the Association of Legal Administrators (ALA) and asked them to share their related tips, experiences and concerns via an online survey and subsequent one-on-one interviews. For each area of analysis, I've also provided an "action item" regarding what you can do now to better manage data security in your firm.

PHYSICAL SECURITY

Less sophisticated security breaches, such as data physically stolen from your premises, are much more prevalent than high-tech hacker break-ins. Do you know who has access to your systems, including night staff and landlords? You need to assess how secure your building and office equipment truly are.

A lot can be learned about the realities of physical versus virtual security by looking at a recent Experian study on identity theft. Only one in 10 cases of identity theft occurs due to online activity. Physical, on-site risk is much more prevalent.

To get an idea of how seriously law firms need to consider physical data theft, consider the practices of ALA member Richard A. Massaro, Systems and Technology Manager at a 70-person firm in Philadelphia, Pennsylvania:

"Our servers are behind locked doors, and only three people have access to them," said Massaro. "An alarm will go off if the door is opened, notifying the police. There's also a motion sensor for the alarm. Most access is over RDP (Remote Desktop Protocol), so the server room is pretty much off-limits. It's not even labeled. Most people don't even know it's there."

Action Item: *Assess physical access to machines and devices where sensitive information is stored. Put locks, alarms and other measures in place to avoid data removal.*

SOFTWARE SECURITY

If your firm has contracted a software developer to develop a custom solution, you need to have someone on your side who is knowledgeable about web threats. Defenses for common attacks, such as SQL Injection or cross-site scripting, need to be built into the software code from the ground up. Good developers with a keen awareness of security issues are versed in a discipline called "thread modeling," which takes these attacks into consideration. Some due diligence will reveal their level of comfort with writing secure code.

One immediate red flag is if your developer writes his or her own login, authentication or authorization code. Instead, he or she should rely on standard code libraries, which have already been written and extensively tested to defend against easily exploitable weaknesses.

In any case, you can hire individuals or companies to "attack" any software you build. Security audits can help to identify weaknesses in applications. One company that provides this service at a reasonable price is McAfee through McAfee Secure.

Action Item: *If you haven't already, probe your developer's sophistication and understanding of threat modeling. Hire a security audit consultant or company to evaluate the safety of the code.*

SYSTEM SECURITY

How often do you apply security patches to your servers? When the Cornficker worm infected computers last year, it was able to spread to thousands of Windows-based machines even though Microsoft issued a patch for the exploited vulnerability months ahead of time. If you don't want your firm's computers to be infected with viruses or worms, make sure you apply patches as soon as you verify they won't disrupt your network.

Malicious botnets, or groups of computers under remote control, seem like the stuff of science fiction, but they are a black-market reality. There's a solid chance your computer is a soldier in an army of zombie computers, infected via worms or viruses and sending out spam on behalf of those willing to pay.

Kevin Driscoll, Director of IT at a Midwestern U.S. law firm, maintains several approaches to look for and eliminate such programs, known as malware or spyware. "I look at the Processes tab under Task Manager to show people what's running when they turn on their computers, and they'll see pages and pages of running programs."

He recommends running up-to-date malware removal programs such as SpyBot or Malwarebytes, but he cautions to change these programs yearly. Cyber-criminals constantly evolve their attacks based on the vulnerabilities of market-leading malware removal programs, so IT professionals need to stay ahead of the curve.

Aside from security patches and malware removal, viruses are always a constant concern. Maintaining up-to-date virus detection and removal programs – such as those provided by Norton, McAfee or AVG – is a critical component of system security.

System security often starts with e-mail, one of the main sources of viruses. If your firm can afford a

Larry Port, *Chief Software Architect*, ROCKET MATTER

Aside from **security patches** and malware removal, **viruses are always a constant concern**. Maintaining up-to-date virus detection and removal programs – such as those provided by Norton, McAfee or AVG – is a **critical component** of system security.

dedicated spam filter appliance, such as a Barracuda or DoubleCheck NMGI, it's worth the cost.

"We were getting 150,000 e-mails a week, and 95 percent of them were spam," said Massaro. "After we implemented the DoubleCheck box, 5,000 e-mails got through, all legitimate. It sits in front of Exchange and saves us a ton of money and time. It works for outbound e-mail, too, so if one of your machines gets taken over, it will kill the message."

Action Item: *Make sure your servers are patched within 30 days of issuance. Maintain up-to-date malware and virus protection. If possible, use non-market leading hardware. If you can afford it, invest in a dedicated spam appliance.*

MOBILE SECURITY

In 2003, a Morgan Stanley Vice President of Mergers and Acquisitions sold a company BlackBerry device on eBay. As one might surmise, the device contained highly sensitive e-mails and contact information. As absurd as it sounds to sell such a device on eBay, what happens in your firm if something more mundane happens? What if, for example, a smartphone is lost?

BlackBerry Enterprise Server (BES) allows IT professionals to remotely wipe data off a device. That's a great thing if your firm is large enough to afford BES (roughly 20 attorneys or more) and has BlackBerry standardized as a mobile platform. However, now that iPhones, Droids and Palm Pre devices are in widespread use, administrators now face a heterogeneous mobile environment.

Supporting a broad array of mobile devices presents two problems. First, BES cannot be used to automatically disable every lost device. Second, smartphones get personalized, by varying degrees, by their owners. When an IT professional resets a password for e-mail, it can cause numerous integration problems on the device. This means pressure on IT staff, lost time and frustration.

What measures can be taken?

"We try to limit the kinds of activities attorneys are doing on their mobile devices," said Driscoll. "They're more of a scheduling and communication messaging platform. If a mobile device is lost, we immediately reset passwords on e-mail. The devices are password protected as well."

Action Item: *If you haven't considered the risk of losing a mobile device, consider the confidentiality of your e-mail. Come up with standard procedures and measures, such as using BES, changing passwords immediately and locking down devices with passwords.*

REMOTE SECURITY

In reality, mobile devices represent just one form of remote access. When considering remote access, the end goal is to limit the scope of activity and access to the office servers. Driscoll and Massaro both said their firms are very selective in terms of who gets remote access and what kinds of things they can do.

"The more I keep [remote devices] to being just a keyboard and a screen and I keep the CPU cycles on my side, the better for me," said Driscoll.

Internal servers and information should be accessed from outside the network via an encrypted channel tunneling through a firewall. Virtual Private Networks (VPNs) are common, but they are not the only mechanisms for secure tunneling. Firewalls provide IT staff with access logs that can be examined for intrusion detection and serve as an audit trail. Remote users should not be able to map drives on machines outside the network to machines inside the network; rather, straight remote desktop sessions should be used.

When granting access to machines in the network, avoid giving anyone the role of Administrator.

"No one is assigned the role of Administrator aside from the Administrator itself. Logouts are forced after extended periods of time," said Massaro.

Action Item: *Identify who has remote access into the systems and what they are authorized to do. Limit these activities as much as possible. Limit remote machines to nothing more than keyboards and monitors.*

DATA BACKUPS

Data theft is one category of disaster, but data loss or corruption can be equally catastrophic. Information deemed critical needs to be backed up at least daily and ideally several times a day. Keeping backup copies at the same location as the originals creates a problem if the office is unavailable or destroyed; as such, storing off-site backups is a critical element in any business continuity strategy.

Fortunately, backing up data these days is inexpensive and easy. One gigabyte of storage typically costs less than 25 cents. Online backup services, which have favorable ethics opinions written about them by multiple bar associations, offer reasonable rates for unlimited offsite encrypted storage. Amazon S3, Mozy, Carbonite and others all offer reasonable turnkey remote backup solutions.

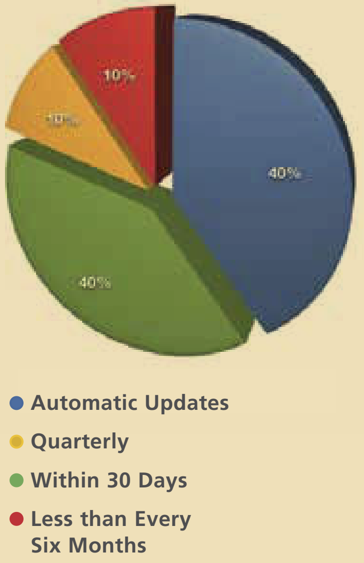
For those IT professionals not included to consider remote backup, a strategy comprising tape backup for longer term, richer data, coupled with disk backup, which offers more immediate

WHAT IT PROFESSIONALS ARE DOING NOW ABOUT DATA SECURITY

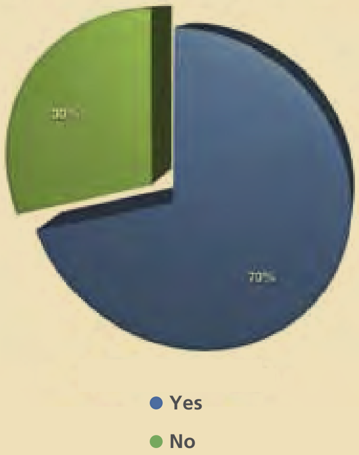
BY LARRY PORT

In conjunction with writing this article, I contacted IT professionals who are also members of the Association of Legal Administrators (ALA) and asked them to share their data security tips, best practices, experiences and concerns via an online survey. Here's a snapshot of the results of some of the most important questions:

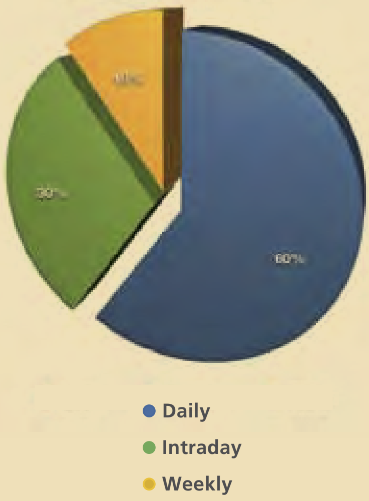
How often do you patch your servers?



Do you backup your data to a secure, offsite location?



How often is your data backed up?



yet less detailed information, can provide law firms with business continuity.

Action Item: *If you're not backing up mission critical information at least daily, get moving. Pick up a dedicated backup drive, such as Netgear ReadyNAS, or sign up with an encrypted, reliable online backup service.*

PASSWORD POLICIES

An IT manager can maintain a bulletproof network only to fall victim to someone choosing "12345" as his or her password. If someone can gain access to a system by a password hack, then all of the firewalls and similar mechanisms in the world cannot keep them out. Maintaining a firm password policy is as important as a firewall.

Said one survey respondent: "We use a strong password policy requiring a minimum of eight characters and two out of three of alpha upper case, alpha lower case, numbers and characters (!@#$%^&*()). Users are prompted to change their passwords every six months."

Using numbers and special characters eliminates dictionary attacks, through which the intruder runs through all words in a dictionary to gain access to a system. If this sounds preposterous, remember how fast computers are and what they're capable of doing in one second. Another layer of protection restricts common passwords (the most common of which is, ironically, "password"). Twitter made "banning predictable passwords" news recently when it posted a list of prohibited, frequently used passwords. As much of a hassle as it may seem to change one's password every six months, it's well worth it.

Action Item: *Assess your organization's current password policy. Make sure you eliminate common passwords, put complex rules in place for password creation and force users to change them every six months.*

CLOUD COMPUTING

If, by now, you're adding up the time and cost of security initiatives and are scared of your growing to-do list, an alternative exists in outsourced, web-based solutions that manage security concerns for you.

"Cloud Computing" is also known as "Utility Computing." Law firms can plug into the internet much as they can tap into the power grid for electricity. Instead of power, they consume software for electronic data discovery, e-mail, document management, matter management or time and billing needs, typically by using a web browser over an encrypted channel ("https").

If (and this is a big "if") a firm chooses the correct cloud provider, it will be able to leverage physically secure and continually audited data facilities, redundant backups, secure connectivity, constant monitoring and server security. The advantage of using a good cloud provider is that firms can leverage IT resources they could not otherwise afford.

However, not all cloud computing providers are created equal, so it's up to each law firm to conduct thorough due diligence and inquire in depth about the provider's data security policies.

Action Item: *If you are interested in using a web-based software solution, investigate the data security policies of candidate cloud providers.*

WHY IT MATTERS

In our highly networked world, it's critical to be on guard with a battery of ammunition to steel your law firm against the cold, harsh reality of data intrusion. A short article such as this cannot cover all topics of data security, but it can serve as a starting point.

In terms of evading cyber attacks, it's a constant cat-and-mouse game. The most important thing to know is this: We all need to keep learning. ❇

about the author

Larry Port is the Chief Software Architect for Rocket Matter, a technology company providing web-based software for the legal profession. Contact him at *larry@rocketmatter.com* or via Twitter (*@rocketmatter*).