

Bar the Digital Door: Securing Your Systems

David Whelan
Director, ABA Legal Technology Resource Center

Introduction

Code Red. "Black hat" hacker. Denial of service. A daily barrage of nicknames and slang are a constant reminder of the growing threat to your data. The security of a computer network has never been more important and yet the most basic preventive measures are often neglected. This problem is caused, in part, by the increasing oversight of computer networks by non-technical staff and management. As your staff and leadership become increasingly educated about the use of technology, they should be constantly assessing the security of your network.

Bar associations may not appear to be traditional targets but as your organization connects up to the Internet for the first time, you can open yourself to increased possibilities of harm. Why would a bar association be a target? One reason might be that associations capture membership data. Add to that data credit card or bank account numbers, disciplinary information, background checks for bar examinations, and other confidential data and it becomes clearer that each association's network can be a treasure trove of information.

There can be a tendency, in light of recent terrorist attacks and disasters, to feel that these dangers only occur in extraordinary circumstances. It is important not to be overwhelmed by the potential dangers. It is equally important not to underestimate them, due to the hype every "cyber attack" garners. It is true that viruses and hackers are constantly probing for vulnerabilities but it is just as likely that your data backup will fail or your server hard drives will be zapped by an electrical surge.

Many of the potential threats to your organization will come from the inside, as a recent ad campaign by eTrust Security attempts to underscore.¹ These are often unintentional but can be no less damaging. Mitigating their effects can sometimes raise trust issues within an organization. It is important that security not be treated as a "we trust X but not Y" issue. Rather, everyone should be educated about the potential dangers and that, in some cases, it is better for some not to have unnecessary access than risk inadvertent damage.

There are simple steps that you can take to begin to harden your organization's defenses and prepare to avoid attacks, from both the outside and the inside. It is worth splitting the security issue into two segments: the physical threats and the virtual threats.

¹ "You're protected against hackers, viruses, and worms. But what about Rose in Benefits?" Computer Associates eTrust Security Solutions advertisement, Information Week.

Physical Threats

Physical threats involve the ability of your hardware to be accessed and damaged or compromised. While not as sexy as being hacked, there are many elements to consider when you turn on your computers and link them together in a network.

Electrical

The uninterruptible power supply (UPS) is one of the great inventions that has come to support the computer world. A UPS is more reliable than a typical surge protector in that it modulates the current it receives to ensure that an electrical spike does not damage your equipment. A surge protector will choke off a spike but, depending on how sensitive it is, will still allow some amount of that spike to reach your server. It is a roll of the dice as to whether that amount is sufficient to damage your hard drives and other network hardware. A UPS absorbs the spike and continues to distribute a measured amount of power to your computer. In the event of a power outage, it can continue to power your server, sometimes up to an hour, allowing you to properly power down your computer without data loss.

Data Redundancy and Backup

Associations live or die based on their membership. As you gather more and more information about these important people, it becomes imperative to safeguard the data using backup and redundancy tools. They can be protection against all manner of disaster. Backup is the act of storing a copy of your data and important programs on removable media and then removing it. Redundancy involves using extra hardware within a computer to make a backup truly a backup.

Redundancy

Merriam-Webster defines this as "an instance of needless repetition".² Redundancy, when discussing computer data, refers to the use of additional hard drives to "mirror" your primary hard drive. This "mirror" drive contains the exact same content as your main hard drive, reflecting each deletion, addition, and change. If something happens to your primary hard drive, you can swap it out and put in the "mirror" and you are immediately back up and running.

The most basic level of redundancy is to use "dynamic disk" mirroring. This involves two hard drives (hence the "mirror") and software that manages the relationship. For Windows servers, the operating system controls the mirroring. This redundancy is also known as redundant array of independent disks, or RAID. Mirroring is also known as RAID1, because it uses 1 extra hard drive. The optimal goal is RAID5, where your server has 6 drives, 5 of which are involved in creating a redundant copy. How much redundancy you use will depend on how much you can afford, with RAID5 costing more than RAID1. The higher the RAID number, the more reliable your redundancy is. It is

² Merriam-Webster Online Collegiate Dictionary <<http://www.m-w.com>>

Bar the Digital Door: Securing Your Systems

not implausible for both drives in a mirrored set, or RAID1 array, to fail simultaneously. It is much less likely that 3 or 5 or more disks would do so.

Backup

Even more important than redundancy is the vigilant backup of your data. It is a process that can be almost entirely automated and is the one business process related to your data that can make or break your association. Businesses that perform regular, methodical backups and store that data off-site are going to stand a greater chance of surviving a crisis, whether foreseeable like a fire or unforeseeable like a terrorist attack.

The essence of a backup routine is that it is (a) done every day, including weekends, and (b) that the backup media, containing the stored data, is removable. Small organizations may have sufficiently little data that it can be stored on a rewritable CD. Larger organizations would want to use tapes to backup their data. Keep in mind that data backup is distinguished from data redundancy by the fact that a data backup is typically more selective than redundancy. When you mirror drives, the redundant drive has a full copy of every file on the primary drive. With a backup, you can pick and choose selected software and data.

Backups are easiest when they are automated. Your backup software, built into most Windows operating systems, should run at night when the network is used the least. Each morning, the tape or other removable media should be taken away from your organization's offices and replaced with a new tape. Someone in your organization should be given the permanent responsibility for ensuring tapes are changed, not re-used too soon, and then removed from the building.

A common failure of the organization that has performed a backup procedure is to test the tapes. If you perform backups on a regular basis, and the tape whirrs and clicks, and you remove it and insert a new tape, you still cannot be sure that the tape you removed has anything on it. Every so often, you should test a tape to ensure that (a) it has data backed up on it and (b) that you can restore data from the tape. If you cannot, then you are in no better position than if you had not backed up at all.

Hardware Accessibility

One of the most obvious threats to your network is made possible by how accessible your hardware is. A basic network consists of:

- Computers, both those used at the desktop and those that act as servers, providing access to data and printers and the Internet;
- Network wiring or wireless communications paths;
- Network hardware that manages communications, including routers, gateways, and hubs.

Bar the Digital Door: Securing Your Systems

Desktop Computer Access

Desktop computers should be turned off and should require passwords either (a) when they are first started or (b) when someone tries to access them. Every person using your network should have her own unique password and username. These should be kept private and not written down.

The Problem with Passwords

It is a common statement that the longer and more complex a password, the harder it is to break. And the harder it is to remember. Balancing complexity and ease of recall can be tricky. It may be better to have a slightly easier password - although still not a proper name, dictionary word, or date - that can be memorized without being written down. If you have an impossible-to-crack password, you may guarantee that it will be written down. It is probably more important that the password be changed on a regular basis. If it is changed often, then you can avoid some of the harm caused when a password is broken, since the new password will block the unauthorized access.

Servers Are a Different Animal

It is hard to do anything about physical access to desktop computers. The fact that they are regularly used can impede unauthorized access. Servers are a different story. In general, no-one needs regular access to the physical server computer. Leaving a server computer out in the open is an invitation for problems, intended or otherwise. A server can be unplugged and carried off. It can be knocked off its stand and broken. An ecologically-minded staff person may turn it off at night, when it should be backing up the association's data. A server computer should **always** be placed in a locked, cooled room to which few have access. Even better, the server's room should not have any windows or clues as to what it holds.

Routers and Hubs and Firewalls, Oh My

The rest of the network is subject to the same analysis. If the network hardware is big enough to be noticeable (and most of it will fit in a bread box), you should enclose it in a locked room or cabinet. You generally cannot do anything about your network wiring but at some point the wire comes up for air at a network port or jack. This is where your computers, servers, and printers are plugged in. Be aware that they can be unplugged and an unauthorized computer can be put on your network that can "sniff" data, break passwords, and otherwise cause havoc.

Hardware Care

This may be somewhat unfamiliar terrain but network hardware needs some coddling. The placement of your network technology - server(s), routers, hubs, etc. - is incredibly vital. Accessibility was discussed above. Environment needs also must be considered and can be the easiest to overlook.

Heating and Cooling

Network servers should be in climate-controlled rooms with air conditioning to avoid overheating. Their rooms should be large enough to allow for airflow.

Bar the Digital Door: Securing Your Systems

Water

Unlike most every other room in your organization, avoid placing sprinkler systems over the server. In the event of a fire, they might indeed put out a fire in the server. Alternatively, in a test or accidental activation, they could cause your equipment to short out, causing irreparable physical damage to your hardware and data. Clearly, you should have some fire control mechanism. If it is a sprinkler, attempt to place your server in a position least likely to cause accidental damage by water.

Water from above is not the only threat. You may also be susceptible to flooding. If your equipment is in a ground floor or lower room, elevate your computers and hardware, and their power and network cords, to keep them above any potential flood water.

Virtual Threats

The computer threats most commonly reported in the news are the virtual threats. These are attacks and probes that come across the wires from remote locations. Many of these will target your bar association by chance and you can best protect yourself by closing as many doors to them as possible.

Viruses and Worms

One of the most insidious threats to any network are the increasing number of viruses and worms that are making the rounds. These are programs that, when executed, can wreak havoc. Typically they are received as e-mail attachments. The primary difference between the virus and the worm is that the worm's "payload" will not generally cause damage to your files – instead, it will complete some other action, like e-mailing itself to all of the people in your e-mail address book. The worm can sometimes include a "Trojan Horse" which is a program that hides itself until timing or a command activates it.

You can protect against them by using anti-virus software on every computer – desktop and server – in your association. Most anti-virus software can be configured to update itself automatically. Additionally, if you have the software installed on your servers, you can often use the server to "push" the anti-virus updates to the desktop computers in a way that is transparent to the user.

Even with anti-virus software, though, your users will be exposed to viruses. The software can only protect against known viruses and so should not be considered a 100% reliable protection. Recent attacks have begun long before any anti-virus companies could protect against them. The second component to anti-virus protection is user education. Your staff should be educated on which attachments to open and which to avoid. They should understand that a much higher level of caution should be exercised when (a) a message is sent to them with an attachment that does not seem work related and (b) the file does not end with a typical document extension -.wpd or .doc.

Bar the Digital Door: Securing Your Systems

The only way to remain virus-free is to be exceptionally vigilant. Since the effects of activating a virus can be damaging to your internal data as well as your association's reputation if your computers are used to attack others, it is an extremely important process and, thankfully, one that is largely within your control.

Intrusions and Firewalls

Network intrusions are an additional way hackers will attempt to compromise your security. Intrusions may be by design or hackers may happen upon you by chance. Some intruders will have selected your network on purpose – they may have an idea of how to attack your systems or expect certain data to be available there. Others will use “war dialing” or “port scanning” techniques that will cause them to stumble across your network when vulnerabilities are found. The most effective thing you can do is to make your network invisible to the latter and be vigilant about the former.

First, you can secure your modems. In many computers, you can use a modem to dial out to the Internet or to receive and send faxes. These modems are often configured so that when an external caller contacts them, they will automatically answer. Hackers use a technique called “war dialing” to automatically dial long lists of phone numbers. When a phone number responds, they make a note of it and can attempt to connect to it and break in later. If you have modems connected to a phone line, make sure you have turned off their auto response feature. If you need to have a modem respond to an outside caller, only turn on the auto-response feature when it is needed.

Next, you can secure your network via its routers and other network hardware. Every server has a number of ports so that when other computers send requests – to deliver e-mail, to access a Web page, etc. – they send the request to a specific port and the server responds. When a server is first installed, it has many ports activated so that you can get started quickly. Unfortunately, some of the ports create vulnerabilities and should be turned off. The SANS Institute and the FBI have created a list of the top 20 vulnerabilities in Windows and UNIX servers.³ The first one is to turn off all default services and port access that are not being used.

You can also add a firewall to your network. A firewall provides a barrier through which all requests pass – both those from the inside and those from the outside. Each request is checked to verify that the data being sent and the port being used are available. Incoming requests are blocked if they are not correctly directed. A firewall can be configured so that ports that are closed are invisible to outsiders. This defeats another hacking technique called port scanning. This is done like “war dialing”. A computer's Internet address is identified and then all the port numbers are checked one by one. When a port responds, it can then be actively investigated and possibly hacked.

³ <http://www.sans.org/top20.htm>

Bar the Digital Door: Securing Your Systems

These should block most casual intruders. A determined hacker will not be dissuaded by firewalls and other security measures. You may not be able to afford the level of security protection required to block their access. You can, however, monitor your systems to ensure you know when your network is being probed. Your firewall maintains an access log that will show when someone has attempted to connect to your network. Your servers maintain security access logs that can help you see when someone is attempting to log in and fails. Other applications, like Web servers, will have their own access logs and you can again see what resources are being requested and by whom. In the case of viruses like Code Red and Nimda, you can see when an infected computer contacts you because all of the requests via the Web server are logged.

Remote Attacks

The last type of intrusion to watch is the type Code Red generated, a remote attack. In truth, all of these virtual attacks are remote. This is different in that your computers are not hacked but someone else's is. That computer is infected with a virus or a program is installed by a hacker that starts to automatically attack other computers. Some of these programs are created to merely generate requests from other computers. The program generates so many requests that the server is overwhelmed and no-one else can request any resources. This is called a denial of service attack. The hacker is no longer present but she has left another computer to do her dirty work.

Conclusion

There are many potential threats to your network systems. Fortunately, many of them can be secured with little additional effort or expense on your part. Education of association staff, vigilance on the part of your network administrators, and continued interest by association leadership in both the security of your data and the reputation of your association are vital to the continued success of your organization.