something that most small CPA firms find overwhelming. And, if they don't find it overwhelming they aren't paying attention. Attacks are no longer just email viruses that ...

Sep. 26, 2016

The cyber-threat landscape has evolved considerably over the last 5 years into something that most small CPA firms find overwhelming. And, if they don't find it overwhelming they aren't paying attention. Attacks are no longer just email viruses

that can cause down time. The focus of modern attacks are on financial fraud and

Whether you have in-house IT staff or use an outside provider you need to assess their security knowledge. Do they understand the current threat landscape? Do they keep up with security news from inside and outside of the CPA industry? Do they take responsibility for security training within the firm? These are critical questions. You must have a frank discussion with your IT manager or provider to discuss their security understanding. If it is lacking, you must consider supplementing with an outside security consultant.

Once a security knowledge worker is in place on behalf of the firm, you can focus on strategy. We can imagine CPA security risk as a pyramid, with the bottom being the most likely to occur and the top being the least likely.

Currently, we can construct the risk pyramid like this:

Seeing the risk laid out like this helps to identify what defenses can overlap to give the biggest return on our security investment. For example, it would make little sense to spend 75% of our time and money on firewalls and adaptive security appliances when all of the firm's laptops are still unencrypted. The likelihood of an attacker directly breaking into your network over the wire is much less than just a common laptop theft or loss.

Instead of going through these risk levels and talking about mitigations to each threat, we can solve it with a layered approach, where each layer covers a large area of the risk pyramid and overlaps with the others so that there is no single point of failure.

The layers:

1. **Antivirus/encryption** – What used to be called "antivirus" has now evolved into a suite of products called "endpoint protection" that can protect your workstations

from many types of threats. Every workstation should also employee full disk

5. **Strong password policies** – Enforce strong, unique passwords and make it a firm policy that this password is not to be used for anything other than computer login. Other network-level access passwords such as VPN's should be different.
6. **Firewall content filtering** – Even small firewalls now offer filtering of different categories of content. At minimum, "advertising" and "recently registered domains" should be blocked.

These six layers apply to all of the highest risk cyber threats a firm will face, and they are all critical parts of the puzzle. No single layer can stand on its own, and none can be left out. Of course, there are many other layers you can implement to enhance your security beyond these. But, these six should be considered a baseline implementation for every sized firm. If you don't know for sure that your firm has these in place, I suggest you print this out and give it to your IT Manager, or schedule a meeting with your IT provider and tell them you want these layers in place.

The last thing you need to do is come to terms with this: Nothing can stop a sufficiently motivated, highly skilled attacker with enough time from breaking into your system. Cyber-security is not about absolute protection because that's impossible. It's about layering your defenses so that your firm is no longer "low hanging fruit". Most hackers are not "highly skilled". Those are rare. So, getting yourself out of that bottom rung of exposure should be the goal.

———————

Dave Jones is the IT Manager for Pearce, Bevill, Leesburg, Moore, P.C in Birmingham, AL. He has been a network and system administrator in the Birmingham, AL area for 19 years. He has been in the CPA technology field for 17 years.

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us