Avoid These Three Common Security Blind Spots

As an IT Consultant, I often see firms unknowingly putting their business information at risk in small ways. Whether this is due to a lack of awareness of firm security policies or simply a lack of security restrictions, the simple fact is that most firms could do more to protect their data. While implementing a firewall, a spam filter, and a password policy is a great start, much more is needed in the way of education, awareness and workflow to completely protect a business from today's evolving threats.

Below are three common blind spots that, if left unchecked, can be a huge risk to security or client confidentially.

1. Open Downloading

Most firms have no policy or restrictions in place for downloading content off the web. This is risky because not everyone understands how to identify what is safe to download. Someone may think they are downloading Dropbox, but are actually downloading malicious software. If your firm doesn't have restrictions in place to prevent employees from downloading programs, at least be sure to include something in your employee manual to make them aware of the risk.

2. Document Sharing

How often do you email documents directly to clients as email attachments? Did you know attachments are sent in plain or clear text? Basically, this means that someone with the know-how could capture the email in transit and read it. Start thinking about what those documents contain; bank account numbers, SSN, contract information. You can easily see how this is a risky practice.

Do your employees have a secure option to share documents? If not then remember, "life, uh, finds a way." If your firm is not providing a secure sharing option, staff members will likely come up with their own way.

Many firms have a disconnected Frankenstein's monster solution for document sharing. Some use Dropbox while others use Google Drive. While both are secure solutions (when used correctly), they do not provide the firm the ability to administer, audit, or review who shared what with who. Additionally, keep in mind that allowing the use of different document sharing programs is also a security risk. Mixed solutions increase the surface area for attack.

In many cases, even the Office Managers and Partners don't know what programs are being used or how to access them if needed. When left unmonitored, the firm has no oversight over what is being shared. Keep in mind that these programs may also prohibit productivity and efficiency - which affects profit! To resolve this, I recommend instituting a firm-wide solution for external document sharing that works in both directions. This could be something like a portal though your practice manage system, Citrix Sharefile, Dropbox for Business, or an integrated DMS portal. Just get everyone on the same secure platform and train them on how to use it properly.

3. Unencrypted Email

Not all important and confidential information is sent as a document attached to an email. Sometimes the important and confidential information is in the email itself! Institute a firm with option for sending encrypted email. Most firms I work with don't even know this is an option. Does it make sending and receiving emails a bit more difficult? Yes. But it's worth it to protect important information. Keep in mind, some solutions offer the ability to choose which emails are encrypted.

Work with your IT consultant to determine how to close these security blind spots and setup policies to manage them going forward. This will reduce your risk and prevent your staff from finding a way to do these things on their own.