The Fulcrum Group, Inc.
(817) 337-0300

Evaluating Your Company's IT Security Strategy

8 Things Small Businesses Can Do To Tighten Up Their IT Security

This White Paper is brought to you by your friends at The Fulcrum Group, Inc.

THE FULCRUM GROUP
One Technology Solution: Yours

The Fulcrum Group, Inc. 5600 Egg Farm Rd., Suite 452, Fort Worth TX 76244
Phone: 817.337.0300 Fax: 817.337.0313 Help Desk: 817.898.1277
info@fulcrumgroup.net www.fulcrum.pro

Security From A Risk-Management Perspective

As seasoned technology specialists, as well as business owners, the years spent in our field have shown us that computer and network security is less a technical issue than it is a risk management concern. This is best seen in the same light as other management issues, such as driving revenue, expense control, inventory or staffing. Conscientious management seems to best support solid security efforts.

Not just a "small business problem", remember extremely large organizations are being compromised, in increasing numbers.

In addition to a firewall and anti-virus tools, large organizations tend to deploy a host of other tools for multi-layer protection – sometimes referred to as 'defense in depth'. Like an onion is protected by layers of papery skin, an appropriate number of complementary security tools (versus a single tool) more thoroughly protects your users and your data.

Tools such as web filtering, smarter firewalls, intrusion prevention and various others are great, but getting yourself off "the wildebeest list" (a nod to 'Mutual Of Omaha's Wild Kingdom' I utilized as a security metaphor in the May edition of our newsletter, available on our website) should also be priority. Briefly, being the last wildebeest in the pack guarantees an easy predator takedown. Don't be that guy, in security terms.

Besides the basic firewall and anti-virus, there are low cost things you should do in attempts to work yourself into the middle of the herd. For SMBs, good focus is to make sure we consistently implement all the lowest costs tools and processes first.

Here are 8 Things You Can Do Right Now To Tighten Up Security In Your Organization:

1) Establish guidelines for how users should act on the network, referred to as **policies and procedures**.
Use policies and procedures as blueprints to try and help you determine what to protect and how to protect.

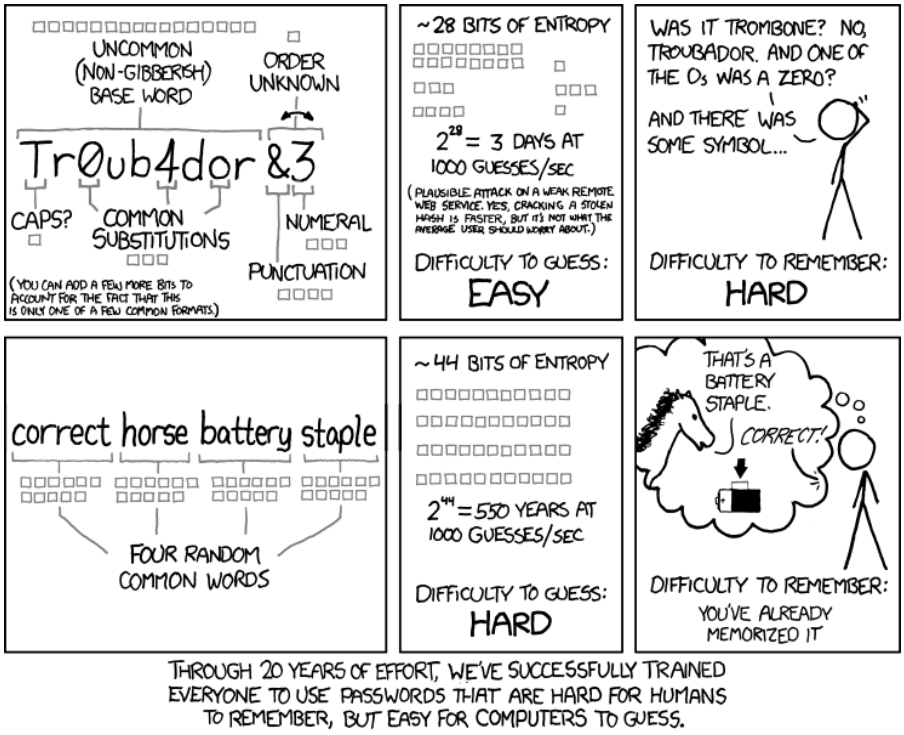
2) **Thorough configuration** of your **lowest cost solutions** - including regular patching of your PCs, laptops and servers - is our recommendation.
Remember that devices like firewalls, printers, switches and others have firmware updates that can add more protection against attackers.

THE FULCRUM GROUP
One Technology Solution: Yours

The Fulcrum Group, Inc. 5600 Egg Farm Rd., Suite 452, Fort Worth TX 76244
Phone: 817.337.0300 Fax: 817.337.0313 Help Desk: 817.898.1277
info@fulcrumgroup.net www.fulcrum.pro

3) **Longer or more complex passwords** cost nothing but can help prevent easier access.

Modern thought is it is better to have a complex pass *phrase*, like "heyletmeintothenetwork" instead of (even an intricate) single word, "L3tm31n".



4) **Take advantage of freebie procedures** -including file system permissions, not logging in as an Administrator for day-to-day work, and/or using Windows Group Policy.

These can help enforce behaviors on users, browsers and so forth.

5) **Update** your applications.

Your line of business applications might have issues but some attacks are based on the freeware foundations of Adobe Acrobat reader, Flash, Shockwave – even your browser might be insecure. These seem small but can reduce the ways attackers try and get an in.

6) End users should make owners or IT personnel aware of any **needed cloud applications**.

Recent newsmaking vulnerabilities have been exposed around such applications as DropBox, EverNote and a host of other cloud applications. Great apps, but, as any, they are also open to certain vulnerabilities, such as we saw recently with the Heartbleed Bug. IT Management needs to be aware of the applications you and other employees are using to help determine if there is any potential risk. By all users speaking up, you could discover that using these apps makes sense for the whole company and at the same time, your IT may know a way to stay protected and allow everyone to have access.

7) **You are only as secure as your least secure connection**.

What may first come to mind is VPN users or business partners, however a network user could accidentally allow access by poorly configured wireless at home, picking up and using an unknown USB drive or bringing an infected/unprotected laptop into the office (behind the firewall).

8) All the tools in the world won't protect you if users aren't aware of **good, basic security habits**.

The most common way malware can get in these days is from email attachments or links within emails. Hopefully, most of us in IT are aware that clicking a link can install software ('malware') – be certain all your system users are aware, too. HIPAA and other security compliance programs stress Security Awareness training for this very reason.

THE FULCRUM GROUP
One Technology Solution: Yours

The Fulcrum Group, Inc. 5600 Egg Farm Rd., Suite 452, Fort Worth TX 76244
Phone: 817.337.0300 Fax: 817.337.0313 Help Desk: 817.898.1277
info@fulcrumgroup.net www.fulcrum.pro

You can take a McAfee's quiz at https://phishingquiz.mcafee.com/ to see how aptly you (and your employees) can spot phishing emails.

It is growing more and more critical to have a proactive IT team on your side to protect your business, your users, and your data from compromise. The Fulcrum Group is your IT team. Our array of managed services assists businesses of all sizes in aligning IT needs with business strategy and implementing the right procedures and tools for your organization's safety.

If you would like more information on how to ensure the security of your business, feel free to reach out to us at info@fulcrumgroup.net .