

# THE PROBLEM SOLVER

"Insider Tips To Make Your Business Run Faster, Easier, And More Profitably"

## What's New

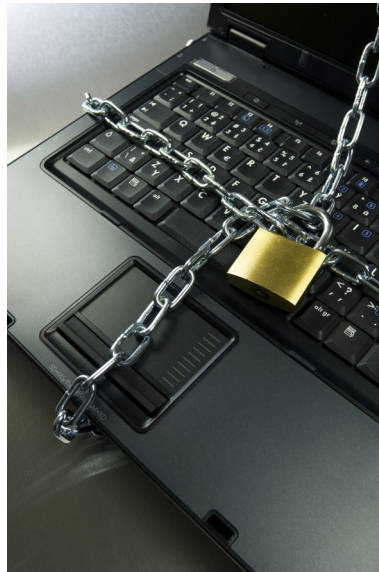
Late last year, we notified clients that Intel Security had plans to decommission McAfee SaaS Email Protection (formerly MX Logic). We're now happy to announce that, after careful evaluation, we're moving to Proofpoint as our email security tool of choice. Proofpoint offers the best combination of features and advanced technologies to identify more threats and stop them before they enter your organization. With Proofpoint, clients continue to enjoy spam/virus protection and email continuity, and can now upgrade to include encryption and archiving services. Contact us for details.

## February 2016



This monthly publication provided courtesy of Simon Tutt, President & CEO of DP Solutions.

"As a business owner, you don't have time to waste on technical and operational issues. That's where we shine! Call us and put an end to your IT problems finally and forever!"



## Worried About Your Network's Security?

*You should be, unless somebody's keeping a vigilant eye on it for you...*

**N**ot too long ago, in a place not so far away...when ancient hordes attacked your city, a single breach in the wall could mean certain death – or at least the end of life as you know it.

Yet times change...or do they?

Attacks by today's cybercriminals on your network, while perhaps not physically life-threatening, can inflict severe damage to the life and health of your business.

**FACT:** The odds of a successful cyber-attack against your business today are one in five. And, at a typical cost of \$300,000 or more, a full 60% of smaller businesses that suffer a breach shut their doors for good within six months, according to the National Cyber Security Alliance.

So, who's "guarding the gate" at your company's network?

The problem with keeping your network safe today is that these

attacks don't just happen randomly – they are constant and unrelenting. Ever more sophisticated "robot" software is making it easier than ever for attackers to stalk the Internet, probing for vulnerabilities 24/7.

Here are just a few of the ways these vigilantes can penetrate your network's defenses:

**An SQL Injection** can destroy your database, steal e-mail addresses, usernames and passwords, gain access to sensitive client management and billing data, deface your web site and defraud your business. It's also now the most frequent mode of attack.

**Open Ports** – An open port is basically a channel for Internet data to connect with devices on your network. A firewall normally filters data, but hacker "web-bots" constantly probe for vulnerabilities. When they find an open port, and if they have installed malicious code inside your system, *they are then able*

Get More Free Tips, Tools and Services At Our Web Site: [www.dpsolutions.com](http://www.dpsolutions.com)

(410) 720-3300

to control your devices.

In a **DDoS attack**, a network of computers attacks a single server with a surge of traffic, forcing it to crash. They most often target political organizations and banks; however, small businesses are also at risk. To avoid getting shut down, you need a defense plan in place and around-the-clock monitoring.

### Malware and Viruses –

Unfortunately, anti-malware and antivirus software programs in reality often fall short of claims, leaving many SMB networks highly vulnerable. The problem is twofold: First, they only detect a breach after the malware or virus has infected your system. Second, detection solutions often lag behind the latest threats by days or even weeks, leaving a big window for them to inflict heavy damage.

*“They most often target political organizations and banks; however, small businesses are also at risk.”*

**Targeted E-mails** – Cybercriminals seem to get better each day at creating enticing e-mails that innocent readers will click on without a moment’s thought. If that reader happens to be on your network, you now have yet another hidden attacker to deal with.

**“Drive-By Downloads”** are a client-side intrusion where a person in your network innocently picks up a nasty bug...

**Credit Card Theft** – How would you feel if one of your customers’ credit cards got hacked due to a flaw in your security? Now imagine how you would feel if

that incident turned into a lawsuit... Yet that is exactly what can happen if your DLP (Data Loss Prevention) system isn’t up to snuff. As you’ve no doubt seen in the news, credit card data theft is now epidemic. To keep customer data safe and maintain PCI compliance, it’s absolutely crucial to make sure your DLP is on duty 100% of the time.

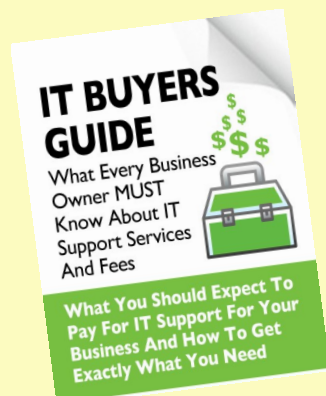
As cybercriminals (and foreign government agents) hone their evil craft, we must now be on guard, as our businesses grow ever more web-dependent. Yet how do you find the time to keep up with it all, much less make sure your network is safe?

### Lucky for you, there’s a silver dagger...

Call us and receive a FREE “Network Health Scan” for a personalized report of recommended improvements to keep your network safe. **Claim yours now at 410-720-3300 or [www.dpsolutions.com/network-health-scan](http://www.dpsolutions.com/network-health-scan).**

As the Guardian Small Business Network states in a January 2015 article, **“Hiring experts to ensure your IT systems and web site are secure makes sense**, as does picking the right payment provider and educating staff.”

## Free IT Buyers Guide: What You Should Be Paying For IT Support & Services



Ever wonder what you **SHOULD** be paying for IT support? Curious to know what type of support plan is the most cost-effective? This new report will answer those questions and reveal:

- The three most common ways IT services companies charge for their services, and the pros and cons of each approach.
- A common billing model that puts **ALL THE RISK** on you, the customer, when buying IT services; you’ll learn what it is and why you need to avoid agreeing to it.
- Exclusions, hidden fees and other “gotcha” clauses IT companies put in their con- tracts that you **DON’T** want to agree to.
- How to make sure you know exactly what you’re getting to avoid disappointment, frustration and added costs later on that you didn’t anticipate.

**Get the Free report at [www.dpsolutions.com/ITbuyersguide](http://www.dpsolutions.com/ITbuyersguide)**

## Client Spotlight: Foundation Fighting Blindness

The Foundation Fighting Blindness (FFB) is paving the way for finding a cure for blindness. This national non-profit organization is devoted to driving research to provide preventions, treatments, and cures for those impacted by retinal degenerative diseases. FFB currently funds over 134 research studies, 71 prominent research institutions and eye hospitals worldwide, including 15 dedicated research centers.

With so much life-changing work at stake, it's critical that FFB's technology be robust and reliable enough to support the invaluable research that drive its' mission. FFB uses cutting-edge technologies, such as a Virtual Desktop Infrastructure (VDI), to provide staff across multiple locations throughout the U.S. with efficient, reliable computer systems. VDI also simplifies their internal IT administration, allowing them to spend less time addressing support issues and more time supporting organizational initiatives.

To learn how you can join the fight to end blindness, visit [www.blindness.org](http://www.blindness.org).

## How A Twist Of Humor Took The "Sting" Out Of A Situation

**A** couple of years ago I had the opportunity to address the Drug & Alcohol Testing Industry Association. It was one of the most memorable programs I have done in my career; the people attending the conference provide drug & alcohol testing for any company, organization, state or federal agency.

During my interviewing process with them, one of the questions I asked was ... "What makes your job difficult?" Several people responded: "Having to deal with all the stupid excuses people give for testing positive for drugs." That response really intrigued me, so I dug deeper in my questioning to get actual examples of their excuses; I will get to the excuses in a moment.

To help make their jobs easier, I suggested a different approach. I proposed they print up a little one-page list of excuses that will not be accepted for testing positive for drugs and hand that to them before being tested. That way, if they do test positive for having drugs or alcohol in their system, there is no need to waste everyone's time using any of the excuses listed.

Below are the actual excuses given (with NO embellishment) and the form I suggested they print up.

### **Excuses That Don't Work for Testing Positive for Drugs You Will Need To Try Something Different – These Aren't Acceptable More Originality Will Be Required**

- ◆ I was at a party and everyone was smoking pot around me, so it's second-hand smoke.
- ◆ Someone must have put something in my drink; I swear I would never

use drugs.

- ◆ I take my friend's pain meds when I have a migraine.
- ◆ I used to smoke pot years ago when I was fat. I hear it stays in your system for a long time.
- ◆ It was the cookies I ate at a party. I think it was medical marijuana.
- ◆ I ate a bunch of poppy seed muffins.
- ◆ I kissed a girl who had just used cocaine.
- ◆ I take supplements from the health food store.
- ◆ I buy hemp oil and make salad dressing with it.
- ◆ I have to light my wife's joints for her because she uses medical marijuana and she is too sick to do it herself.

So now, when someone tests positive, they no longer have to deal with these 10 silly excuses ... hopefully saving them a little time and frustration. And they did it by adding a little twist of humor in the process.

As a leader, try taking a look at things you have to do, like: evaluations, reviews, critiques, changing policies, implementing new software, meeting deadlines, revamping procedures, enforcing guidelines, delegating responsibilities, giving feedback, or complying with government regulations ... and see if you can find a different approach that might make it be accepted more favorably.

Originality and humor can help take the "sting" out of any situation, so anytime you can add a little of it, to help take the drudgery or negativity out of an issue, mandate, or task... I recommend you go for it.



Robert Stevenson is a highly sought after, internationally known speaker. He is the author of the best-selling books *How to Soar Like An Eagle in a World Full of Turkeys* and *52 Essential Habits For Success*. Robert is a graduate of the Georgia Institute of Technology (Georgia Tech) and is a former All-American Athlete. He started his first business at 24 and has owned several companies. Robert has international sales experience dealing in over 20 countries, and his client list reads like a Who's Who in Business. He has shared the podium with such renowned names as Generals Colin Powell and Norman Schwarzkopf, Former President George H.W. Bush, Anthony Robbins and Steven Covey. [www.robertstevenson.org/](http://www.robertstevenson.org/)

## Your Employees

■ **Here are a couple of key things Virgin Group founder Richard Branson** does to make sure he brings in the best people:

*Don't delegate this critical task.* Branson likes to get his hands dirty in the hiring process. Especially at the top level, nobody knows better than you who's a good fit – and who isn't.

*Put character first, résumé second.* Branson sometimes has applicants play games or tell jokes to let their personality shine through. Often, you'll get more insight from real-life interactions than from words on a page.

Adapted From *3 Rules From Richard Branson for Hiring Remarkable People* by Zoe Henry in Inc.com

## Your Marketing

■ **Here are three ways to WOW your customers** – and turn them into raving fans...*Be sincere.* Notice little things and show genuine interest. Observe and use what you see to connect. Making sales is easier when you first make friends. *Ask questions...lots of them...* Listen and your customer will tell you what they need. And knowing that is the shortest path to an easy sale. *Know your product.* What's unique about it? What fun facts can you share? Bring those facts to life and you gain not just the sale – you win over a customer.

Adapted from *7 Ways to Wow Your Customers* by Nicole Smartt on [Business2Community.com](http://Business2Community.com)

## Your Money

■ **A recent survey from Bank of America and Braun Research** found that 70% of small business owners are concerned about the costs of providing health care coverage. After all, even budget-minded plans can be pricey. So what can you do?

Regardless of how you may feel about the Affordable Care Act, take advantage of the way it promotes employee health. Create a wellness program that rewards employees for embracing healthy behaviors such as losing weight, quitting smoking and eating well. A 2012 AFLAC report showed that wellness programs can reduce sick days, health costs and workers' comp claims by 25% or more.

Source: *Bank of America Small Business Owner Report*

## Your Office

■ **Here are three tips from the ancient art of feng shui** to make your office more productive – and less stressful...

1. Place your desk with a solid wall behind you, so you can see the room's entry. This enhances your sense of control and confidence.
2. Get rid of clutter. An uncluttered space leads to clear thinking and reduces stress.
3. Replace fatigue-inducing fluorescent lamps with natural and incandescent light.

Tungsten and halogen lamps, too bright for direct illumination, can be reflected off walls and ceilings for an energy-efficient source of daylight spectrum lighting.

Adapted from *The Practical Encyclopedia of Feng Shui* by Gill Hale

## Your Security

According to the Ponemon Institute, 69% of data breaches are caused by insiders. Compare that to just 16% caused by outside intruders. Here are three things you can do to combat this threat. First, make sure that identities and passwords are changed regularly. Second, guard closely against unauthorized use of credentials. And finally, human error is the leading cause of insider data leaks. Build and monitor systems that are more or less "fail-safe" and can withstand human errors. Of course you want to trust your team, but today's realities dictate that it's up to you to keep a watchful eye.

Adapted from *Five Steps to Preventing Insider Data Breaches* in IT Business Edge

© MAZIK ANDERSON, WWW.ANDERZTOONS.COM



"We're still not sure what happened here, but I think we can all agree that we're glad it's over."