TMC's ADVISOR

Covering IT and Telecom from a Western Canadian Viewpoint — *January 2015*

How The World Sees You Issue

Just When You Thought You Were Safe—Fighting Spam

By Peter Aggus

In the last issue we reviewed how attackers disable internet access with a torrent of unwanted IP traffic. Mail servers, of course, can be attacked in a similar way but the solution here seems easier – spam filtering. Be warned, however, that spam filters can have serious unintended consequences.

Read More

Inside

Early Warning Indicators - By Alan Bajkov

Life is change and as the pace of change mounts, available reaction time decreases. The world may love your company one day, then consider it to be a poor performer on the next. Neither economists nor fortune-tellers can deliver reliable predictions of the future so you need to identify a range of early warning indicators to buy a little extra reaction time.

Is Google Really My Friend? - By John Glover

In the October issue we examined Google and how it operates as a co-owner of your content and stores your deleted content forever. Today we address a continuing debate about whether individuals are entitled to "anonymity" to protect their personal privacy and to preserve their identity. Social media providers' drive for profits from your data is leading to a drive for control of social media by government.

How Others See Me - By Ellen Koskinen-Dodgson

When a certified business coach joined TMC, I jumped on the chance to have her work her magic on me. It's always fun to be analyzed and 'find out' what type of person you are. The process seemed straightforward enough and I knew what the process would say about me because I know what type of person I am. Well, apparently not.

See You There

Ellen will be speaking at the 16th Annual Privacy and Security Conference (February 12th and 13th) at the Victoria Conference Centre.

She'll be on a panel about the Internet of Things at 11 on Friday morning.

The conference, is recognized as one of the top tier information privacy and security events in North America. It draws an international audience of some 1,000 delegates with an interest in cutting edge policy, programs, law, research and technologies aimed at the protection of privacy and security.

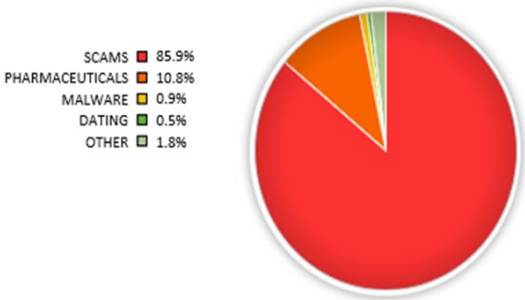
Fighting Spam and the Laws of Unintended Consequences

By Peter Aggus

In the last issue we reviewed how attackers disable internet access with a torrent of unwanted IP traffic. Mail servers, of course, can be attacked in a similar way but the solution here seems easier – spam filtering. Be warned, however, that spam filters can have serious unintended consequences.

No-one Wants Spam

Physical ad-mail is expensive but it's almost free to distribute bulk email. Thus we live with the scourge we know as 'spam'. Some say that their email systems process more spam than valid mail. Enter spam filters. Unfortunately, these can work with varying levels of autonomy which is where the problems come in.



Spam Filters

Spam filters are widely used by companies trying to reduce their email processing, storage and archive costs. While filters do work, they can block legitimate mail and actually increase the cost of doing business.

Some filters simply look for virus signatures in mail and attachments. These are a great way to firewall a business from email based virus attacks. Some filters go further and try to recognize patterns of text that often indicate spam. Unfortunately the same patterns are found in legitimate mail. Consider a typical subject filter based on 'Do you have…' designed to stop those scam e-mails trying to sell you things you do not want. Now think what happens to a legitimate email using a good business technique of putting the question into the subject field.

A filter can be set to simply tag mail and send the end user a warning. It can also be set to block mail and tell no one. Worse, it won't reply to the sender since replies often encourage more spam by confirming that an address is valid. The sender will not know that their mail wasn't delivered. Since email counts as a legal communication, your spam filter could even cause legal problems.

A filter can be given even more autonomy. It can send 'unsubscribe' messages to senders to stop the further transmission of email from that source. The sender sees this as a legitimate request but the intended recipient has no idea what was done.

Blacklisting

Another way to hamstring spammers is to report their IP address so it can be blacklisted. ISPs use these lists to stop torrents of spam at source. However, when the spammers realize that their IP address has been blocked, they simply refresh their dynamically assigned address and get a new one, leaving the old blacklisted one to be assigned to the next unsuspecting user. If you have ever cursed your cellular supplier when an outgoing mail fails, this may explain things.

Gmail

Did you know that Gmail now sorts incoming mail so not all of it ends up in your inbox? If all you read is your Inbox then, like spam filters, this can result in the loss of legitimate mail.

Best Practices

ISPs should refresh IP blacklists after an hour or so but sometimes they need to be reminded. Gmail settings should be checked. Corporate spam filters should be set to block only virus-infected mail and to tag other questionable mail, leaving the decision to keep or delete to the person to whom the mail is addressed. This includes auto-unsubscribes.

This article is reproduced from the January 2015 edition of ***TMC's Advisor***

Peter, as an engineer and technology management consultant, has developed innovative and cost-effective solutions for clients in many industries.

Early Warning Indicators

By Alan Bajkov

Life is change and as the pace of change mounts, available reaction time decreases. The world may love your company one day, then consider it to be a poor performer on the next. Neither economists nor fortune-tellers can deliver reliable predictions of the future so you need to identify a range of early warning indicators to buy a little extra reaction time.

Everything Changes

Every industry and sub-industry is faced with new opportunities and with failure risks every day. The IT department can implement systems that look to the future through executive dashboards. Dashboards come in many forms and can flag changing risks and opportunities through early warning indicators.

	Today	Next Q	Next Year
Economy			
Industry Trends			
Competitors			
Sales			
Image			
Risk			

Identify Red Flags

The most often cited sources of early warning indicators are planning, budgeting, scenario building, scanning, conferences, peer group meetings, inspection, monitoring reports, surveys, research and governance systems. Unfortunately, numerical analysis can take you only so far and by the time the events are recorded on the financial statements, it may be too late. You need to determine what's likely to drive the behaviour of customers and markets.

The best source of early warning indicators is simply to ask management across all departments as well as front line staff and other stakeholders. They will identify sources including:

- Regional and national economies
- Developments at key competitors
- Global trends in your industry
- Trends based on increasing numbers of online and mobile customers
- Reputation changes as tracked by complaints and social media
- Changing patterns of customer communications
- Staff satisfaction
- Enterprise risk
- Internal performance changes
- Testing customer response to potential products/services
- Other sources that are specific to your industry

Easier Said Than Done

Developing a comprehensive set of early warning indicators is a major exercise. As an example, in measuring staff satisfaction, there are 7 – 10 factors that are crucial to the final rating. By examining the causal factors that influence each of the core factors, early warning indicators begin to appear. Each category has many layers and components and each component needs to be accurate and appropriate.

Once a dashboard or other reporting system has been established, it needs to be used and kept up to date. Boards and senior management need to decide if they should allocate a few minutes at each meeting to review early warning indicators. IT management should take charge of keeping the system up to date. At a minimum, they should maintain a register of all components that feed into the system and when each needs to be reviewed. They should also regularly survey staff and stakeholders to ask which indicators are currently important.

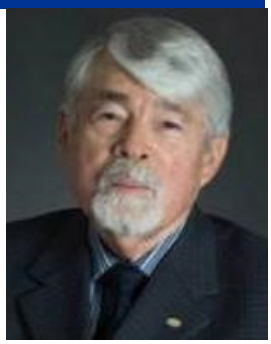
The objective of an early warning indicator dashboard is to track change and interpret its implications. The challenge is to build confidence in the indicators and to act decisively when the need arises.

This article is reproduced from the January 2015 edition of ***TMC's Advisor***

Alan Bajkov is a senior executive professional with over 30 years of experience with enterprise risk management practices covering IT governance and IT project management.

Is Google Really My Friend?

By John Glover



In the October issue we examined Google and how it operates as a co-owner of your content and stores your deleted content forever. Today we address a continuing debate about whether individuals are entitled to "anonymity" to protect their personal privacy and to preserve their identity. Social media providers' drive for profits from your data is leading to a drive for control of social media by government.

The Dark Side of the Net

There is a dark side to this wonderful tool called the Internet and we're reminded daily that information can be a weapon as well as a benefit. Cyber fraud, Cyber espionage, Cyber warfare and Cyber stalking are everyday occurrences in 2015. The 'forever Internet' can damage careers as HR recruiters search the net to decide on the desirability of job seekers.

Not enough is being done by social media providers, search engines and other on-line services to support safe use of this technology. Google and Facebook are such large companies that they get away with setting their own rules.

EU vs. Google

Social Media has come under the spotlight and services like Google are under severe scrutiny by governments and lawmakers globally. On November 27, 2014, European Union lawmakers overwhelmingly backed a motion urging anti-trust regulators to break up Google. This is reminiscent of the break-up of AT&T in 1982 when it was the biggest company in the world.

The Right to be Forgotten

The internet has a long memory. But what if the pictures, data and personal information that it can pull up about you appear unfair, one-sided or just plain wrong? More and more people are claiming they have a "right to be forgotten" and are even trying to delete themselves from the web. The issue appears poised to generate legal, technological and moral wrangling for years to come.

The top European court has backed the "right to be forgotten" and said Google must delete "inadequate, irrelevant or no longer relevant" data from its results when a member of the public requests it. Legal experts said the ruling could give the go-ahead to deletion requests of material including embarrassing photographs and even insults on social media websites which could lead to a rethink in the way they handle links to content on the web.

So What To Do?

1. Remind ourselves about the power and scope of these tools and their dark side;

2. Be cautious of what you commit to the Internet **in any form** or **forum** to minimize the possibility of embarrassment or other negative consequences;

3. Understand and accept that once information is delivered to Internet based information services it is there **forever** unless the "right to be forgotten" can apply.

4. Examine, correct and confirm that erroneous or irrelevant or outdated information is purged with the same degree of thoroughness as one would take with our credit rating at the various credit bureaus. Start by looking up your profile on Google and other social mediums and do the due diligence. If necessary, ask for help.

5. Implement and maintain the basic protection mechanisms that are there to protect your privacy and keep your technology safe. Anti-Virus and personal firewall protection is a minimum with a keen eye on incoming messages or web pages that were not requested.

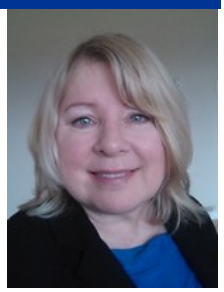
6. Surf carefully and "look both ways when crossing the Net"!

This article is reproduced from the January 2015 edition of ***TMC's Advisor***

John Glover assists national and international clients with governance, IT systems compliance auditing, IT risk assessment, information policy formulation and PCI data security.

How Others See Me

By Ellen Koskinen-Dodgson



When a certified business coach joined TMC, I jumped on the chance to have her work her magic on me. It's always fun to be analyzed and 'find out' what type of person you are. The process seemed straightforward enough and I knew what the process would say about me because I know what type of person I am. Well, apparently not.

An In-house Expert

When Thomi Glover joined TMC, she suggested that I have her conduct a 'Personal Style Assessment' as a way to gain first-hand knowledge of her consulting specialty, Executive and Management Coaching. She explained that I would gain a better understanding of my personal style and that I would learn how to become more successful in my interactions with people. "OK," I said, "but I already know that I'm the analytic type."

The Test Begins

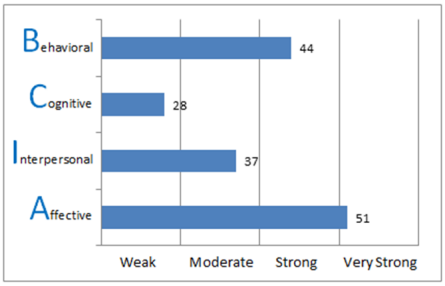
It was simple enough - I logged onto the site and was presented with questions to ask. It started with simple questions. Each question stated 4 management style characteristics and I ranked them from most like me to least like me. Then the questions got tougher and none of the four choices were like me at all.

I started to wonder if the next question was going to ask if I was more like an axe murderer or a torturer. Of course it didn't, but I really had to think before answering.

Since it was an automated system, I got the results quickly and read the results several times. Of the four style types, 'Cognitive' was the closest fit to the analytic type that I knew was me. My lowest score was Cognitive. So much for knowing myself.

Analysis and Feedback

Thomi went through the results with me to help me come to terms with the results and to explain what I should learn from them. My scores were:



It turns out that my combination gives me a primary pattern of 'Idealistic'. This means that, among other things, I'm creative and practical, future-oriented, task focused, trusting in others (sometimes without reason), that people come first and I talk too much.

My secondary pattern is 'Influential' means that I'm good at encouraging a range of people others to work together, though some will see me as too enthusiastic.

When I shared the results with my colleagues, they grinned and agreed with almost every characteristic, particularly the talking. I still think of myself as an analytic, geeky type because I love technology and I want to know how everything works but I really am all of those other things, too.

Reflection

I have a personal style that's fairly informal and leans heavily on humour. It's often well received but when it's not.... Thomi explained how my style can be downright annoying to Cognitive types, but I can, with effort and practice, learn to read the style preferences of others and adapt my approach to make them comfortable. When people are comfortable, they'll put aside their natural scepticism and really listen to what I'm saying. Making people chuckle in a meeting is not enough. Next month, Thomi will explain how she uses this model to help her clients get better results when working with their

This article is reproduced from the January 2015 edition of ***TMC's Advisor***

Ellen Koskinen-Dodgson is President and Managing Partner of TMC IT and Telecom Consulting Inc. She is an IT and Telecommunications Management Consultant, electrical engineer, author, speaker, media resource and Expert Witness.