TMC's ADVISOR

Covering IT and Telecom from a Canadian Viewpoint *May 2015*

The Importance of Planning Issue

Just When You Thought You Were Safe—Falling for Phishing

By Ellen Koskinen-Dodgson

You receive an email from your IT department telling you that they're increasing security, so you need to log in and change your password. You click on the link and comply, and just like that, you've been phished. The email came from cybercriminals, the link and the log-in screen were offsite and you gave them your user name and password without suspecting a thing. Now they're inside your firewall and no one knows.

Read More

Inside

- By Guy Robertson

Just before dawn, an electrical fault starts a fire in one of your branch sites. You hear the news on the radio and your heart jolts - quick, where's your disaster plan? Sadly, when you dig it out, you realize that it's full of impressive words and philosophical statements but it doesn't clearly tell you what to do. If you don't have a practical disaster management plan, here are 6 simple steps that you can follow. Note that basic assess and replace are but two of the steps.

- By Alan Bajkov

The concept of IT Governance can be intimidating, but it's actually very simple. You need it, you can get into trouble if you don't have it, and it's easy to get it wrong, so it's worth understanding. Through a simple Q&A approach, Alan will transform you into a person who 'gets' IT Governance.

 -By John Glover

The Internet of Things (IoT) is the most hyped "emerging technology" today, but the term and the associated technologies are far from new, so why the sudden surge in interest in 2014? There are a number of intersecting factors that are driving this and the opportunities seem boundless. However, every organization has some important preparatory work as well..

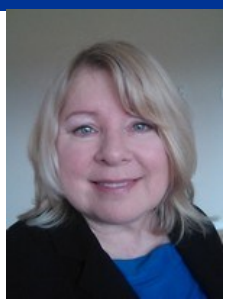
See You There

Ellen will be co-presenting with Assistant Chief Steve Robinson from the Surrey Fire Department at the 2015 BC Fire Expo and Annual Fire Chiefs Association of BC Conference (June 7th to 11th) held at the Penticton Trade and Convention Centre.

They will be co-presenting about the **Planned Reduction of Service Levels during a Disaster** at 7:30am on the morning of Wednesday June 10.

It features the results of an interactive model which was developed to demonstrate the impact on resources and service levels for various emergency events and how policy changes can restore some system capacity.

Falling for Phishing



By Ellen Koskinen-Dodgson

You receive an email from your IT department telling you that they're increasing security, so you need to log in and change your password. You click on the link and comply, and just like that, you've been phished. The email came from cybercriminals, the link and the log-in screen were offsite and you gave them your user name and password without suspecting a thing. Now they're inside your firewall and no one knows.

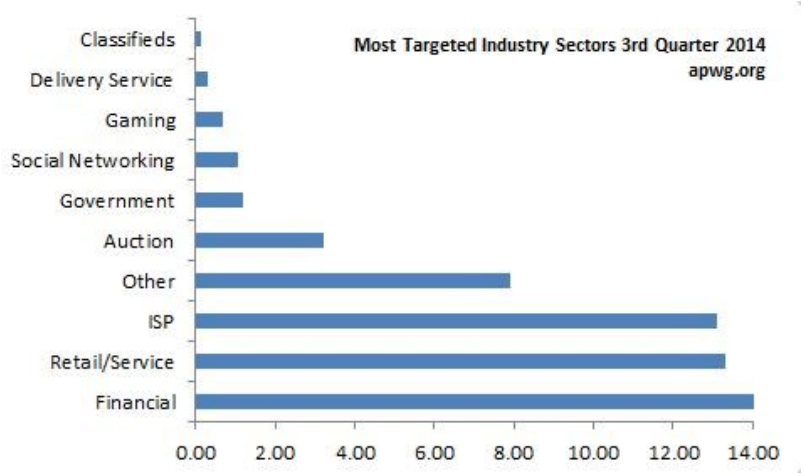
Your Acount Is at Risk!

Phishing (the name was likely influenced by the 80's phone phreaking long distance hacking) can appear to originate from your bank, your credit card company or your IT department. Cybercriminals are becoming ever more sophisticated and no longer sound like the Nigerian scams of old, so you can't depend on the tell-tale spelling mistakes to warn you.

Phish and Whales

It's easy for employees to fall for a phishing attack. The Anti-Phishing Working Group (antiphishing.org) reports that 30,000+ phishing attacks are reported every month with new companies regularly becoming targets. Over 200,000 malware samples are discovered every day and attacks are more sophisticated.

Many attacks are personalized to make them more believable (spear phishing) with some targeted specifically to executives (whales). The jargon makes you smile. The results do not.



Tricky Domain Names

We've all seen misspelled urls and they probably don't fool us anymore. Unfortunately, subdomains still fool many. For example, http://www.mybank.securityupdate.com looks a lot like it would be the security update page of the mybank website when it's actually the mybank section of the securityupdate.com website, which could be anything.

Clone Phishing

This is a technique that uses an infected machine to fool you into providing secure information, exploiting your trust relationship with the sender. The common approach is to send an 'update' to a legitimate email, replacing links or attachments with malicious content.

Clever Pop-ups

The link takes you to the advertised site, so you feel safe. Then a little pop-up window asks for your log-in information. The pop-up window, of course, is not associated with the legitimate site.

What Can You Do?

You need to expect the worst. If you get an email, text or voice call asking for an urgent response, be suspicious. Check before you click. You can hover over the link and view the actual link. Unfortunately this isn't foolproof. The safest way is to call and ask if the request is legitimate, or to navigate directly to the site without using the link. Report suspicious emails to IT.

Of course, the IT department is constantly updating phishing filters and black-listing known phishing sites.

This article is reproduced from the May 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.

Disaster Strikes… "But We're Not Ready!"

By Guy Robertson

Just before dawn, an electrical fault starts a fire in one of your branch sites. You hear the news on the radio and your heart jolts - quick, where's your disaster plan? Sadly, when you dig it out, you realize that it's full of impressive words and philosophical statements but it doesn't clearly tell you what to do. If you don't have a practical disaster management plan, here are 6 simple steps that you can follow. Note that basic assess and replace are but two of the steps.

Step One

Find out if anyone was injured—or worse—in the fire. Enquire about your staff, but also about the firefighters, police officers and the public who might have been at the scene. If there were any casualties, express your concern and condolences. Prepare to manage negative media response and don't make operational losses sound more important than people. Explain how customers will be served in the short term and where branch staff will go.

Step Two

Find out the extent of the damage, and estimate the effects on your organization. Is the location a typical branch location or did it contain systems and equipment that affect the entire organization? If so, identify the most important work and focus on that.

Step Three

Deputize. Don't take on too many responsibilities yourself, or you'll soon be exhausted. Above all, let your more talented and energetic managers rise to the occasion. Rely on them to:

- conduct damage assessments
- prioritize the list of operational problems
- identify options with costs and timelines
- recommend solutions
- talk to suppliers and realtors
- adjust schedules
- deal with individual staff members
- work with customers to minimize their disruption

Step Four

Support your staff. They will look to you for something more than leadership or direction. They'll want you to show your humane side with frequent reassurance as rumours about layoffs might spread. Some staff may take stress leave because of too much work, hectic schedules, confusion and overtime. Encourage staff members to speak openly to you about how they feel, to ask any pressing questions or even with recommendations on how to resume normal operations more quickly. This sort of "verbal therapy", as emergency management specialists call it, can help staff members to obviate doubts and other negative feelings.

Step Five

Normalize. As many staff members can become disorientated after a disaster, focus on resuming normal operations for the majority of staff.

Step Six

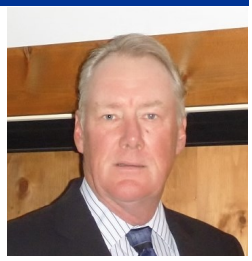
Plan for the future. Even a serious loss of assets should not stop you and your management colleagues from making short-, medium- and long-term plans in a business-as-usual way. Your Board, other authorities and shareholders will be impressed and relieved to see you making progress despite disaster-related disruptions.

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

Guy Robertson is a Senior Management Consultant at TMC who specializes in emergency management and disaster planning. He has written extensively on emergency planning and IT security—hundreds of articles as well as a book with worldwide sales.

IT Governance 101

By Alan Bajkov



The concept of IT Governance can be intimidating, but it's actually very simple. You need it, you can get into trouble if you don't have it, and it's easy to get it wrong, so it's worth understanding. Through a simple Q&A approach, I will transform you into a person who 'gets' IT Governance.

What is IT Governance?

Simply put, an IT governance framework is a way to:

1. ensure that your company stays on track to achieve their strategies and goals
2. align IT strategy with business strategy
3. implement effective ways to measure IT's performance
4. make sure that all stakeholders' interests are taken into account

An IT governance framework should answer some key questions, such as:

1) How is the IT department functioning overall?
2) What key metrics does management need to answer this?
3) What return is IT giving back to the business from the investment being made in IT?

Does everyone need it?

Yes, every organization - large and small, public and private - needs a way to ensure that IT supports the organization's strategies and objectives. The level of sophistication you need to apply to IT governance, however, can vary according to size, industry or applicable regulations. In general, the larger and more regulated the organization, the more detailed the IT governance structure should be.

What is IT's

What are the drivers?

Organizations today are subject to many regulations governing data retention, confidential information, financial accountability and recovery from disasters. This motivates them to implement IT governance infrastructures. While none of these regulations requires an IT governance framework, many organizations have found it to be an excellent way to ensure regulatory compliance. By implementing IT governance, you'll have the internal controls you need to meet the core guidelines of many of these regulations, such as the Sarbanes-Oxley Act of 2002. Of course, it's also worth knowing if IT is providing a positive return on investment (ROI).

Can we do it wrong?

Yes. If the IT governance framework isn't implemented properly, it can directly affect how IT is perceived at a high level. The last thing you want is for IT to be perceived as a cost center that doesn't produce real value. Lack of effective implementation can also cause continued issues with project cost and schedule overruns and poor value to cost measurements, not to mention stakeholder dissatisfaction.

Can we do this alone?

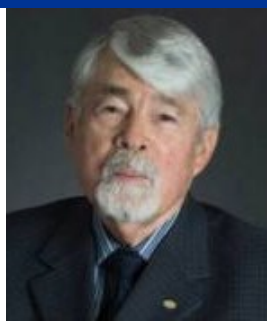
Sometimes it makes sense to get help, and implementing an IT governance framework is one of those times. Not only is internal expertise on IT governance hard to come by, but executives just don't have the time. The best scenario is usually a combination of the two. Internally, someone really needs to own the process, but getting experienced help is essential.

This article is reproduced from the May 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.

The Internet of Things

By John Glover



The Internet of Things (IoT) is the most hyped "emerging technology" today, but the term and the associated technologies are far from new, so why the sudden surge in interest in 2014? There are a number of intersecting factors that are driving this and the opportunities seem boundless. However, every organization has some important preparatory work as well.

Population Explosion

The Internet of Things (IoT) is increasing the connectedness of people and things on a scale that once was unimaginable. Connected devices outnumber the world's population, with the installed base of active wireless connected devices exceeding 16 billion in 2014. By 2020, there are expected to be 41 billion devices connected to the Internet.

Development Drivers

There are a number of intersecting factors that are responsible for this dramatic growth:

The deployment of IPv6 (Internet Protocol Version 6) has provided the opportunity to expand the Internet addressing capability beyond the limitations of IPv4. This has led to a huge increase in IP addressable devices as engineering and imagination have taken hold of this phenomenon.

The price of sensors, processors, and networking has come way down. If Moore's Law is any indication, this trend will continue.

Since Wi-Fi is now widely deployed and supported speeds increasing, it is

relatively easy to add new networked devices to the home, office and industrial plant.

Four major network providers—Cisco, IBM, GE and Amazon—have committed to support IoT with network modifications to support IPv6.

Everyone is excited about investing based on new forecasts regarding the IoT opportunity. GE estimates that the "Industrial Internet" has the potential to add $10 to $15 trillion **(with a 'T')** to global GDP over the next 20 years. Cisco is increasing its forecast to $19 trillion for the economic value created by the "Internet of Everything" in the year 2020.

Adoption Drivers

The pace of IoT market adoption is accelerating because of:

- Growth in analytics and cloud computing
- Increasing interconnectivity of machines and personal smart devices
- The proliferation of applications connecting supply chains, partners, and customers
- This drives most businesses to focus on getting products and services to market more quickly as your highly mobile workforce, customers, and supply chain demand anytime, anywhere business tools.

Getting Prepared

Beyond the normal IoT security cautions, the other big take-away is to speed up your plans to migrate to IPv6. As new IPv4 addresses are all but unavailable, there are many things that will need to be changed to ensure that you remain visible to the rest of the world and gain the full benefits of the IoT.

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

John Glover assists national and international clients with IT governance, IT systems compliance, IT risk assessment, network vulnerability assessments, network penetration testing, information security policy formulation and PCI data security.