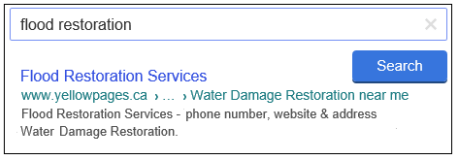
TMC's ADVISOR

Covering IT and Telecom from a Canadian Viewpoint — *July 2017 , Volume 4 Issue 6*

Disaster Planning—3rd Party Relationships are Crucial

By Guy Robertson

A good Disaster Plan is critical for the success of your operations. Everyone knows that. What isn't always as well understood is the importance of establishing relationships and contracts with 3rd party support organizations as part of your Disaster Planning process. The right contracts with 3rd party organizations can be critical for successful business resumption. You may be surprised at our list.



After the flood is the worst time to look for a flood cleanup contractor. If the flood has affected other businesses, you may have to wait weeks before restoration contractors have time to get to you.

Inside

The Sad Truth About Exploits - By John Glover

Let us not be mislead about why we continue to be plagued by exploits related to various IT and control systems in our environments today. We tend to want to transfer the blame to the technology but we need to "fess up" and recognize that we are the architects of our own demise. We are continuing to wring our hands about SCADA and ICS as being the next technical disaster waiting to happen. We believe that the "other" types of business systems are getting the care and feeding that will keep them healthy. Perhaps it is time to wake up and smell the coffee!

Don't Miss The Obvious - By Peter Aggus

When trying to reduce your vulnerability to Cyber Attack, don't overlook the obvious. In our experience, some vulnerabilities are so obvious, that they should never occur, yet they seem to be easy to overlook. We review three examples here - how to improve password security, how to prevent monitoring and unauthorized access to mobile device transmissions, and how to use firewalls for protection within your LAN.

Designing KPIs to Ensure Success - By Ellen Koskinen-Dodgson

Managers need to determine how to define success for their department or organization. They need to answer questions including "How do we define success?", "How do we know if we've achieved success?" and "How do we know if we're headed for a cliff?". IT Management roles increasingly include helping their C-suite executives design the key performance indicators that are the answers to these questions. Here are our top five KPIs.

Your Empty(er) Inbox - Hindsight

July 1 was to usher in a new era of emptier inboxes as the Canadian anti-spam legislation (July1, 2014) moved into the enforcement phase.

Reality? I saw very little change in my inbox.

Conclusion? The email that I get comes from sources that either aren't governed by or don't care about Canada's anti-spam laws.

Impact on the Advisor

For those subscribers that didn't explicitly tell us to continue to send the Advisor and we didn't have a business relationship, we had to drop them from our 'send' list. Our list shrank by more than half!

A Request

I invite you to recommend colleagues to us to add to our distribution list - just provide us their name, position and email address and we'll invite them. You can go to our web site:

http://www.tmcconsulting.ca/admin/subscribe.php

and enter the information there, or send me an email at ellen@tmcconsulting.ca or call Ellen at 604-506-2905.

 ISSN 2369-663X

Disaster Planning—3rd Party Relationships are Crucial

By Guy Robertson

A good Disaster Plan is critical for the success of your operations. Everyone knows that. What isn't always as well understood is the importance of establishing relationships and contracts with 3rd party support organizations as part of your Disaster Planning process. The right contracts with 3rd party organizations can be critical for successful business resumption. You may be surprised at our list.

People First

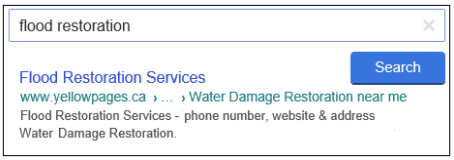
First, make sure that everyone in your workplace is safe. If anyone has been injured, apply first aid and, if necessary, call 911 for an ambulance. However, after a major disaster such as an earthquake, ambulance service might not be available: an excellent reason to make sure that people in your workplace have first aid training.

Outside Help

Make sure that your facilities are stable and secure. Is it safe to enter and exit? If you have any doubts, evacuate the building and do not re-enter it until engineers have inspected the structure.

If your building is safe to re-enter, you can call a disaster recovery firm for assistance. Such firms might describe themselves in different ways, but the services that their teams can offer include:

- Facility inspections for safety and insurance claims
- Post-fire and post-flood clean-up
- Basic repairs to equipment including computers, printers, and photocopiers



After the flood is the worst time to look for a flood cleanup contractor. If the flood has affected other businesses, you may have to wait weeks before restoration contractors have time to get to you.

- Basic cleaning of furniture, carpeting, and curtains
- Restoration of artwork and paper records
- Repairs to plumbing, electrical fixtures, and HVAC
- Disposal of items beyond repair
- Replacement of glazing

While a disaster recovery team works on your damaged facilities and other assets, you should contact (in addition to customers and staff at other sites) the 3rd party organizations that provide services to you:

- Government agencies
- All suppliers to cancel, delay or make changes—when you check, you'll realize that the list is long
- The media and advertisers
- Data centres that provide hosted or back-up services
- Financial services (for payroll, loans, and cash supply)
- Temp services firms, in case any of your employees must be absent
- A security firm for temporary guards if there is a risk of looting

Ideally the disaster recovery team will arrive at your site within two hours (or less) after your call.

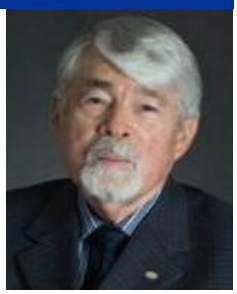
Remember that after a regional disaster such as an earthquake or forest fire, you might have to wait for weeks before teams arrive to assist in you as they might be busy working with customers who had reserved the help as a part of their disaster plans.

As you read this, you must admit that it would be easier to make an comprehensive disaster plan before all hell breaks loose. Why not start now?

This article is reproduced from the July 2017 edition of ***TMC's Advisor***

Guy Robertson s a senior planner at TMC and an instructor at the Justice Institute of BC and Langara College. He has published two books and numerous articles on corporate security and disaster planning, and offered workshops and lectures at conferences across North America and in the UK.

The Sad Truth About Exploits *By John Glover*



Let us not be mislead about why we continue to be plagued by exploits related to various IT and control systems in our environments today. We tend to want to transfer the blame to the technology but we need to "fess up" and recognize that we are the architects of our own demise. We are continuing to wring our hands about SCADA and ICS as being the next technical disaster waiting to happen. We believe that the "other" types of business systems are getting the care and feeding that will keep them healthy. Perhaps it is time to wake up and smell the coffee!

Unpatched Can Be OK

For a very long time now we have been advised that IT systems performing any business or critical functions need to be kept current with software upgrades and patches.

However, we also must remind ourselves that in many cases we are dealing with legacy systems that were functioning very well before they were made Internet ready. There are some older systems that cannot easily be patched. In effect, they are so legacy that they no longer have a custodian and the documentation sucks.

If your systems fall into this category it is still important to keep up to date with **"understanding patches"** - because that will tell you where the risks are known to exist. Apply that knowledge to reducing exposure through some compensating control that is meaningful. Unpatched systems are not a problem, if you do not expose the known risk to exploitation.

Segregation

When these older systems were designed, they were not IP enabled. Connectivity off-site typically used dial-out modems when needed. The

danger comes from combining old and new into a composite network. Once that is done the old system is exposed to risks it was never designed to cope with and the operating system patches needed to add that protection often cannot be applied — particularly with embedded systems or turnkey designs that are under restricted maintenance contracts.

The best solution is often to return to the original design and ask why there was ever a need to expose the old technology to the new environment. It is perfectly acceptable to run two physically separate networks.

Leave your SCADA control network alone and design your modern admin network as a completely separate LAN with its internet connectivity and modern, fully patched Operating Systems.

Duplicating computers where access to both networks is needed is a small price to pay for vastly improved security and peace of mind.

Firewall Lockdown

Where pathways must be added into a legacy network it is vitally important that they are protected by state-of-the-art firewalls that remain fully patched. Lock down everything except what is needed — all the way down to source and destination IP addresses. Pay additional attention to securing the source computers that are exposed to the internet and avoid them being used for general tasks.

False Economy

The dangers of legacy control networks are well known to cyber attackers. The biggest danger is the false economy of 'saving money' by having one network rather than increasing security with two. Pay me up front now or pay me MUCH more later.

This article is reproduced from the July 2017 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.

Don't Miss The Obvious *By Peter Aggus*

When trying to reduce your vulnerability to Cyber Attack, don't overlook the obvious. In our experience, some vulnerabilities are so obvious, that they should never occur, yet they seem to be easy to overlook. We review three examples here - how to improve password security, how to prevent monitoring and unauthorized access to mobile device transmissions, and how to use firewalls for protection within your LAN.

Improve Passwords

It is amazing how many systems still have default passwords. Look at every admin system on routers, firewalls, etc. Don't forget control systems and surveillance systems—the list is long.

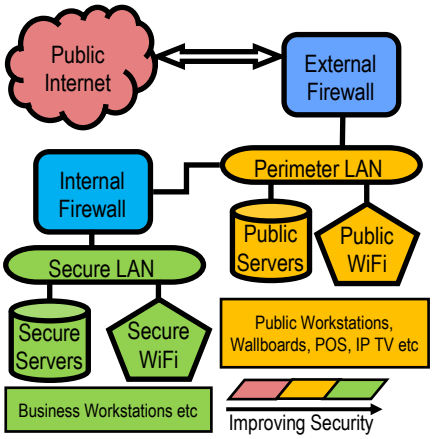
Check your Password Vault to make sure that you have changed the password from the published default...and, of course, change it regularly. Passwords on sensitive systems should be changed every few weeks—general passwords could last 3 months or so.

Educate your users about how to create strong yet memorable passwords. A good way is to:

- create a memorable phrase like 'I Love 2 Scoop Butterscotch Ice Cream In A Waffle Cone'
- generate a complex password by just using first letters.
- improve security by choosing which letter to make upper case
- throw in a punctuation mark to get **iL2sbiciawc!** - which is actually quite complex yet easy for the 'owner' to work out.

Protect Mobile Devices

Most mobile data (whether cellular or WiFi) is not encrypted by default. It is not difficult to do and there are several options.



The simplest way is to use a VPN (Virtual Private Network) service—such that the data path over the mobile link to the VPN server is encrypted. This can be a purchased public service or can be part of a corporate firewall policy.

Firewall Rulebases

Wherever two networks interconnect it is prudent to have a firewall to control access both ways. IT managers know that and firewalls are routinely included between the internet and the corporate LAN.

However good, secure, network design increasingly focusses on partitioning LANs into separate segments connected by routers. This allows sensitive data and systems to be kept away from more general users and, in particular, from WiFi networks that the public has access to. The diagram shows a typical partitioned design.

Business WiFi should ALWAYS be encrypted and the firewalls set to block access from unknown devices. You can still share APs between public and business—just make the business SSID reside on a secure subnet. This is not out-of-the-box design so it needs work by knowledgeable designers.

The High Cost of 'Easy'

Most of the dangers seen at the centre of recent cyber attacks are caused by systems not being designed to be robust but instead being left in their default state.

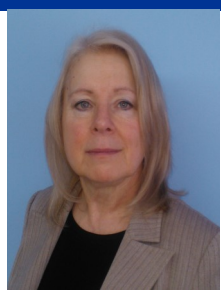
Without encryption, ANYONE can eavesdrop on mobile data—including every password typed. Mobile devices can even be taken over by a man-in-the-middle attack.

Don't take the easy way out—you risk paying a very high price in the end.

This article is reproduced from the July 2017 edition of *TMC's Advisor*

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

Designing KPIs to Ensure Success



By Ellen Koskinen-Dodgson

Managers need to determine how to define success for their department or organization. They need to answer questions including "How do we define success?", "How do we know if we've achieved success?" and "How do we know if we're headed for a cliff?". IT Management roles increasingly include helping their C-suite executives design the key performance indicators that are the answers to these questions. Here are our top five KPIs.

Financial

Financials are the ultimate scorecard because if the financials don't work, nothing else matters.

Financials might include total sales, sales growth or profit. Government or non-profits might measure cost per unit of service.

Customer Experience

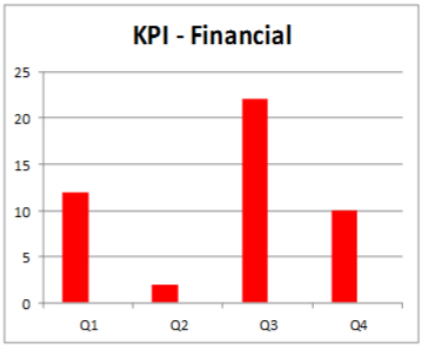
Since your organizational purpose is to deliver product/service to your customers, great customer service is everyone's stated goal. However, the financial KPIs often dictate that money to improve customer service is in short supply.

Customer service improvements are usually driven by coincident cost saving or risk of loss to market share.

Market

Market KPIs compare you to your competitors or measure the changes in the size of your market.

It is sometimes difficult to understand exactly what market you're in. Apple is a great example of redefining their market from the mobile phone market to the smartphone market.



Employee Experience

Everyone 'knows' that having satisfied employees is a good thing. However, the way to achieve a great employee experience generally has a cost associated with it—often higher wages or benefits.

Some sectors intentionally set their wages and benefits at a level that leads to a fairly high turnover rate because they employ a large, unskilled labour pool.

Innovation

Every industry depends on innovation. This is easily understood in the high-tech or fashion fields, but it's also true in every other field. Competitors are constantly working to create improved, less expensive or otherwise more desirable products.

How To Decide?

KPIs can lead a company astray. The following examples illustrate how poorly considered and analyzed KPIs may be misleading:

- Growing sales with decreasing profits
- A growing market share in a shrinking market
- Highly satisfied employees with decreasing profits
- A high market share with low innovation

Data Analytics

While Financial and Market KPIs can indicate current success, there is a delicate balance where declining customer service, employee satisfaction and innovation KPIs can lead to declining Financial and Market KPIs. Data Analytics become ever more crucial.

This article is reproduced from the July 2017 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.