TMC's ADVISOR

Covering IT and Telecom from a Western Canadian Viewpoint *July 2014*

The IT and Telecom Preparedness Issue

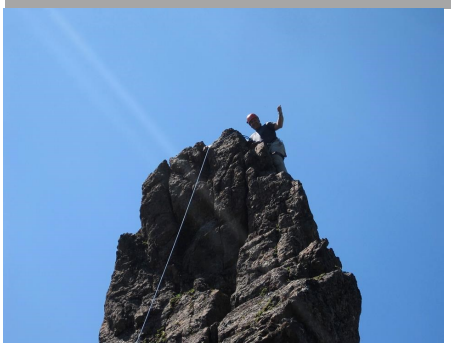


Photo courtesy of Mark Koski

Just When You Thought You Were Safe

By Ellen Koskinen-Dodgson

IT and Telecom Managers think seriously about security and they generally do a pretty good job of it. Having done a pretty good job protecting their LAN and WAN, everyone feels safe. Well, unfortunately our interconnected world is so complexly interconnected that you may find back-doors or even barn doors somewhere in the tentacles of your connections. You'll almost certainly find heating systems or building entry systems or...

Read More

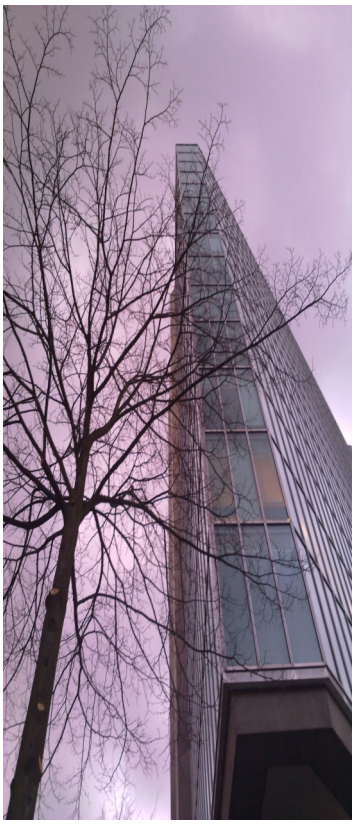
Inside

Check Out TMC and Win!

Over the next year we will be ***giving away*** several ***free*** mini consulting assignments—each ***worth $2,400.***

To qualify, just invite us in to introduce ourselves—and tell us a little about your operations.

Your entry could be pulled out of the hat and could be featured in The Advisor as a future Mini Consulting showcase.



Copyright ©2014 TMC IT and Telecom Consulting Inc.

Just When You Thought You Were Safe — Beware Your Lunch Room Refrigerator

By Ellen Koskinen-Dodgson

IT and Telecom Managers think seriously about security and they generally do a pretty good job of it. Having done a pretty good job protecting their LAN and WAN, everyone feels safe. Well, unfortunately our interconnected world is so complexly interconnected that you may find back-doors or even barn doors somewhere in the tentacles of your connections. You'll almost certainly find heating systems or building entry systems or…

The Risk

Businesses and government offices are full of equipment that has an internet connection but has little or no protection against electronic access. This is also true for many industrial and public infrastructure systems like traffic lights and power generating systems. There are also IT devices that use default admin passwords. These devices are currently protected by obscurity but it's only a matter of time before script kiddies notice the opportunity to wreak havoc. The opportunities for industrial espionage, stock manipulation, evidence planting and public mayhem are also massive.

Shodan

Called 'the scariest search engine on the planet' and 'a kind of "dark" Google' by CNN, Shodan collects information on about 500 million connected devices and services each month. ZDNet calls it 'the Google for hackers'. Shodan's website advertises "Expose online devices: webcams, power plants, routers, iphones, wind turbines, refrigerators, VoIP phones. Find devices based on city, country, latitude/longitude, hostname, IP and operating system.

CNN reports that Shodan has found unsecured controls for security cameras, traffic lights, garage doors, door locks, pressurized water heaters, a hockey rink chiller, a crematorium, a hydroelectric plant in France, and even command and control systems for a nuclear power plant and a particle accelerator. Of course it's good to find security holes so that they can be fixed but how many go unnoticed as there's simply too much to search through?

It's All Very Easy

Shodan has made it easy by archiving previously made searches and making them available for sharing. Their Search Directory is 'the easiest way to get started with finding devices, especially when it comes to locating some of the more obscure things on the Internet'. They even have a mapping interface that will plot your results on a map. If you click on one of the dots, you'll see more information about the device, such as which services it's running, who owns the IP space and anything else that is useful to know. The physical location is no secret.

Non-White-Hat Sources

Of course Shodan is considered to be white-hat and is used by IT departments and penetration testing services but there are Shodan work-alikes that have no restrictions. …and the script kiddie vandals, corporate saboteurs, ransom-ware criminals and other bad guys have barely noticed this opportunity yet.

This article is reproduced from the July 2014 edition of ***TMC's Advisor.***

To receive the Advisor ezine, email:
subscriptions@tmcconsulting.ca

View the Advisor online at:

- **http://tmcconsulting.ca/insights/tmcs_advisor_magazine.php**
- **Or visit our new LinkedIn Showcase Page, TMC's Advisor.**

©2014 TMC IT and Telecom Consulting Inc.

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.

Collateral Damage

By Peter Aggus

A big quake knocks a building down, a smaller one loosens a connector or cracks an aging water pipe. The earth quakes 500,000 times every year and 100,000 of these quakes can be felt … and they happen everywhere. The impact of the event often has a domino effect with failure coming from unexpected places.

What Does It Mean?

What would happen if we were hit by a sizeable earthquake? It doesn't even need to be a devastating one – just a big enough one to disrupt normal business operations. One thing is sure – the bigger the quake, the more unforeseen consequences will occur.

Apart from the immediate effect for days or even weeks, what about the long term consequences on business? Could you recover or are you out of business? The answer depends on how well you have planned for disaster and that means understanding the effects of a disaster on business in the short, medium and long term.

Water Damage

Most businesses will evacuate with everyone else and will return days later – but to what? Broken water mains and in-building piping can make buildings uninhabitable with computers, telephones and paper files virtually a write-off. The carpets are wet and begin to turn moldy. Every restoration company is booked beyond capacity. It isn't safe for staff to occupy the offices.

No Electricity

Underground electrical transformers may have burned or been incapacitated in another way. Downtown is without power so you would need your own generator in order to operate. Hopefully your generator wasn't damaged from the quake or the subsequent water leaks or fires.

No Staff

Your staff is dealing with damaged homes, no schools for their children, problems finding food and gas. They may not want to come to work.

No Network Services

An earthquake can cripple or destroy data and telecom networks. Existing services may be lost. New or replacement services will be difficult to obtain as everyone will be in the same boat. Cell towers may be standing but most do not have backup generators.

No Customer Data

Your IT staff were unable to restore any of the backup data files. Your backups were locally stored rather than off-site. Can you advertise that you want customers to tell you what you are doing for them and whether they owe you any money?

Back To Normal?

Suppose you survived and rebuilt your offices. The insurance company paid to replace everything within your office. Power is operational. Network services are restored. Your staff have returned to work.

How long have you been off-line? What have your customers been doing, especially the ones that weren't affected by the quake? Sadly, they've been buying from your competition. After a major event like an earthquake, a great many businesses do not survive.

Backup Sites

If you had designed your operations to work from multiple cities, part of your operation would have been out of the quake-affected zone and much of your operations would have continued. From a client standpoint, it would have been business as usual except for the delays caused by staff shortages.

This article is reproduced from the July 2014 edition of ***TMC's Advisor***

©2014 TMC IT and Telecom Consulting Inc.

Peter Aggus is Vice President of TMC IT and Telecom Consulting. His Business Continuity training enables him to quickly assess an environment and identify failure points, often failure points that have never previously been identified.

Self-Assessing Enterprise Risk

By Alan Bajkov

Assessing risk is not rocket science; it's a logical process of identifying risks and opportunities, deciding on their likelihood and magnitude of impact, then deciding on an appropriate response to each. The value of a self-assessment process is the learning and fair challenge that this can present to participants: Board of Directors, executive management and line staff. This assessment is often project managed by IT managers.

The ERM Process

1. Linking risk management to enterprise and business unit goals/objectives.
2. Considering risks from all sources – not constrained by organizational boundaries.
3. Matching external impacts with internal realities, e.g., cost, management time.
4. Processes which:
    - identify significant risks;
    - measure significant risks;
    - assess significant risk impact/tolerance;
    - define the appropriate responses to significant risks;
    - monitor significant risks as well as the adequacy of responses; and
    - report on significant risk management effectiveness.
5. Is a coordinated/integrated effort.
6. Is integrated with the strategic planning and governance processes. In a mature model the process would aggregate risk across the entire organization to assess the enterprise risk profile in relation to its capacity to absorb the risk.

The Self-Assessment

1. Provide training session for Board and senior management on Standards and principles of ERM
2. Obtain project approval
3. Develop ERM policy
4. Obtain ERM policy approval
5. Appoint a "self-assessment committee"
6. Develop project plan
7. Facilitate team members' assessment of compliance to each criteria within the policy, documenting evidence of compliance. Where not compliant, outline an action plan to gain compliance. This will take multiple sessions.
8. Independent review of self -assessment
9. Remediate deficiencies if any with team members
10. Report implementation progress to Board or senior management

This article is reproduced from the July 2014 edition of ***TMC's Advisor***

©2014 TMC IT and Telecom Consulting Inc.

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 Unnecessary Disaster

By Len Garis, Peter Aggus and Ellen Koskinen-Dodgson

Urban myths abound – we are often told that 'an event' causes a disaster but it often isn't true. The 2011 tsunami in Japan did not cause the nuclear meltdown. The real cause was bad planning and very bad activation of an emergency plan.

We're very good at creating emergency plans and we are often good at implementing them when an emergency occurs. However, if the emergency doesn't match the assumptions written in the plan, we often insist on following the plan anyway.

Japan Nuclear Disaster

The Japanese probably lead the world in preparing for the consequences of earthquakes, and their preparations have saved an untold number of lives. Unfortunately, not so on March 11, 2011.

At 2:46 p.m., a 9.0-magnitude quake struck off the coast but the three operating nuclear reactors at the Fukushima I power plant were already in the process of shutting down - seismic detectors had picked up the precursor P-wave tremor. This worked exactly as planned.

The immense quantity of residual heat in the core was expected and planned for, in the same way that the molten core of a steel works furnace has massive residual heat even after the furnace shuts down.

The cool-down process takes days – a factor planned into the shutdown procedure.

Preparations had also been made to supply secure power during the cool-down cycle. Duplicated power feeds were provided, along with batteries and on-site generators with adequate fuel. The earthquake happened, power was lost and generators started, exactly as planned.

Approximately an hour after the earthquake, a 14-metre tsunami swept over the 5.7-metre tsunami seawall, inundated the plant and flooded the standby generators. The batteries in the reactor building did their job and bought eight hours of time to solve the unexpected problem. Again, exactly as planned.

Then reality demanded a change of plan but nobody arranged to bring in a replacement generator until the batteries failed. That's when the extremely hot core started splitting water molecules into hydrogen and oxygen. The lighter hydrogen, of course, rose to the roof level where it eventually exploded and blew the roof off.

Remain Flexible

When organizations don't train their people on their emergency plans they have failures in execution because of lack of knowledge. It is also important that the plan not be treated as an unchangeable set of blueprints. You need a process to deal with the unexpected.

Watch for Part 2 in a future issue.

This article is reproduced from the July 2014 edition of ***TMC's Advisor***

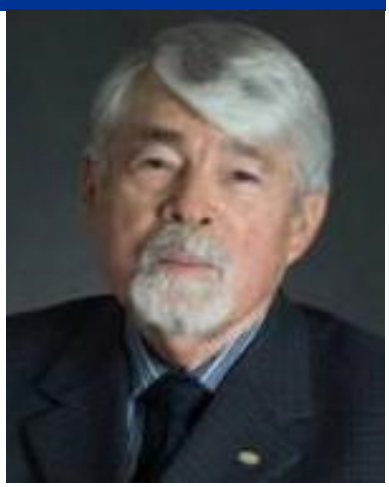
©2014 TMC IT and Telecom Consulting Inc.

Len Garis is the Fire Chief for the City of Surrey, British Columbia, and an adjunct professor in the School of Criminology and Criminal Justice at the University of the Fraser Valley and a Member of the Christian Regenhard Centre for Emergency Response Studies (RaCERS) at John Jay College of Criminal Justice of the City University of New York.

Peter Aggus and Ellen Koskinen-Dodgson are Vice President and President of TMC IT and Telecom Consulting.

You Can Be Sued

By John Glover



Disaster struck and somehow everything is your fault! You were busy; you were understaffed; Governance was on your To Do list. Now it's too late.

Due Care

Organizations of all sizes, even small ones, are expected to exercise "DUE CARE" when conducting their business. Due care is the acceptable level of conduct expected from corporate officers and directors for outcomes that impact stakeholders, clients, customers, employees and society. In fact, if there is a "societal norm" for the organization or enterprise that is not being followed, there is a potential for senior members of the executive and the board to be cited for negligence.

Due Diligence

If advice or warnings of impending problems are ignored, or if there are a lack of reasonable protection mechanisms in place, this becomes an absence of "DUE DILIGENCE". People have been jailed for this and it doesn't only apply to senior members of the executive and the board; it can apply to working level managers!

OECD Benchmark

The Organization for Economic Co-operation and Development (OECD) has created an international convention which has become a recognized and adopted benchmark for policy makers, investors, corporations and other stakeholders worldwide. Many organizations monitor and report on the OECD Principals of Good Governance to ensure that they are providing the due care and due diligence required.

Things Change

In the past, due care and due diligence were held to a much lower standard than they are now. There was a time when an organization was protected by the fact that everyone was going their own way and there were no recognized standard of conduct.

This article is reproduced from the July 2014 edition of ***TMC's Advisor***

©2014 TMC IT and Telecom Consulting Inc.

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