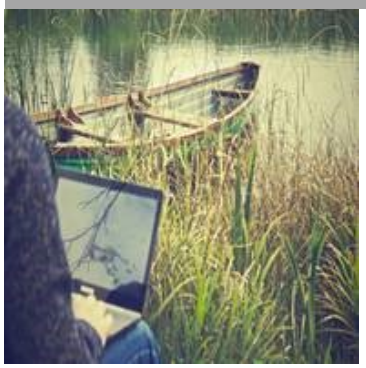
TMC's ADVISOR

Covering IT and Telecom from a Canadian Viewpoint **November 2015, Volume 2 Issue 10**

Customer Service Issue



Just When You Thought You Were Safe - Telecommuting

By Ellen Koskinen-Dodgson

Telecommuting used to be something that just employees wanted. Then it became something that corporations saw as a way to save a lot of money by reducing office space...but it was experimental because they didn't trust their employees. Now it's becoming the way to go for many office jobs and it works fabulously well - until it doesn't.

Read More

Inside

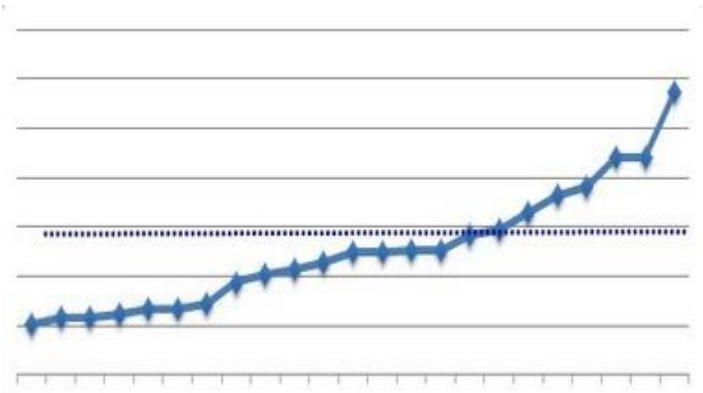
Are You Understaffed?

TMC conducted a benchmarking study of BC municipalities. It benchmarked BC municipalities on a variety of measures including:

- IT spending as a % of revenue
- IT spending per employee
- IT spending breakdown
- IT staffing as a % of corporate staff
- IT workload breakdown
- IT Process self assessment
- Servers and end user device types

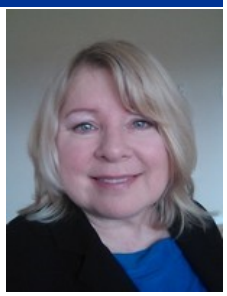
Access your free copy of TMC's ***Municipal IT Staffing Benchmarking Review***

Contact Ellen ellen@tmcconsulting.ca or 604-683-1103.



 ISSN 2369-663X

Just When You Thought You Were Safe – Telecommuting



By Ellen Koskinen-Dodgson

Telecommuting used to be something that just employees wanted. Then it became something that corporations saw as a way to save a lot of money by reducing office space … but it was experimental because they didn't trust their employees. Now it's becoming the way to go for many office jobs and it works fabulously well – until it doesn't.

Stereotypes Debunked

Studies clearly show that the most mean-spirited of the old stereotypes were wrong. Telecommuters are trustworthy.

At least for certain types of work, telecommuting employees are productive, often more productive, and even take fewer sick days.

They experience lower stress, likely because of the lack of commuting, but perhaps because they avoid the interruptions and distractions of a normal office environment.

Though Some Are True

There are many stereotypes that are true and need to be accommodated. These include:

- Opportunities for after-hours socialization
- Less-effective collaboration
- Loss of casual cross-department ideas exchanges
- And the most important, security risks

Accommodations

Most of the shortcomings can be dealt with:

- Socialization can be improved by hosting after-hours get-togethers
- Collaboration can be improved by using better technology or by hosting collaboration retreats
- Casual ideas exchanges can be improved with corporate social media and more hosted socialization
- Security can be improved through:
  - Providing corporate equipment without admin privileges
  - Requiring access by VPN
  - Operating GPS, and remote wipe, on corporate devices
  - Extensive acceptable use policies

But Did You Think of…

Insurance — to protect equipment, files, records, cost of recovery…

Insurance — to protect against a lawsuit from a guest or family member of your employee, where they are injured by tripping over your employee's laptop which the employee left on the lawn of their yard.

WCB — Workers Compensation rates and coverage are based on the assumption that your employees are working at your office in an office-like environment.

WCB Nightmares

Once an employee is working off site, be it at home, in a coffee shop, in a hotel room, or on a row boat, you are no longer in control of their work environment.

Your employees could be operating in a way that would make WCB / the Employment Standards Branch come after you.

This article is reproduced from the November 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.

Cloud adoption: Why Security Risks Shouldn't Stop You

By Peter Aggus

If, like many CIOs, you avoid cloud-based systems because of perceived higher security risks, it might be time to take another look. Many major in-house systems have, in recent months, been shown to have fallible security. Might Cloud Systems actually be better?

The Perceived Problem

Many IT professionals are reluctant to pass responsibility for security to an outside organization. This is understandable because it is still their head on the block if something goes wrong.

After all – if you have responsibility AND you are accountable then you are more likely to do a good job. Right?

Well, that certainly used to be the case but we have recently seen several system hacks that have resulted in spectacular releases of personal information—and all of them were from supposedly secure in-house systems.

Ironically, many IT organizations are less likely to have a high level of expertise in designing and implementing high security than the Cloud Service Providers (CSPs) - who may have more to lose if they get it wrong.

Changes Afoot

Cloud services have been around since 2009. Back then, users had good reason to worry about cloud security risks. CSPs' original focus was exclusively on functionality—emphasising cost savings and scalability. Security concerns were, at best, an afterthought. Recently the approach to cloud security risks has started to change.

> 83% see cyber-attacks among the top three threats facing them but only 38% feel pre-pared to experi-ence one
>
> Source: Global Cybersecurity Status

There are two major steps that CSPs are taking in their efforts to gain customer trust in their security levels.

Firstly, there is a willingness to allow potential customers to conduct assessments of their infrastructure (though you will probably have to press to get your potential CSP to offer such access—like making it a condition of signing up).

Secondly, there is acceptance by CSPs of the need for clients to verify their ability to manage cloud security risks in some certifiable way.

Certification

The American Institute of Certified Public Accountants has introduced what they call the 'Service Organization Control process (SOC)'. Some of the larger cloud service providers like Amazon and Apple now publish SOC reports on their security controls.

Looking Forward

Security is a serious issue, whether in-house or cloud-based. CSPs will continue to improve as they are pressed to do so by their clients. For many users, cloud security may well now exceed what they enjoy internally and so merits serious consideration.

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

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

‘Anywhere, with Any Device’ - Policy Increases Enterprise Risk

By Alan Bajkov

Ignoring top class risk management practices remains an issue for many companies operating in today's global economy. Understanding this fact is crucial, and Boards and educators have a role to play on how best to promote efficient risk management practices within complex organizations and ultimately adapting their training and development programmes to prepare better for problems that arise from a lack of these effective practices.

Compliance vs. Risk Management

In many cases, companies are more concerned with compliance rather than implementing effective risk management. Compliance basically involves following a strict protocol set out by government regulators and other outside regulatory agencies. These protocols always lag behind the realities of actual risk as new risks are constantly emerging. Simple compliance may provide protection from liability but can leave an organization exposed to risk.

Employees

Employees are an ongoing source of new risk exposures. Employees understand that corporations owe them no loyalty so they focus on their own employability and transferability of skills. Promoting employee individualism can go against information sharing and co-operation which is needed to identify and handle risk.

Employees also add risk through their love of technology and their lack of love for security measures. They particularly love the concept of ‘Anywhere, with Any Device’ and are often very creative in their attempts to bypass corporate security policies. The Internet of Things just adds an emerging field of new gadgets that employees will connect to their personal devices and then into the corporate network.

Compliance

≠

Risk

Management

Employee Engagement with ERM

Without employees adopting the right attitude towards risk, this exposure will continue and grow. This requires a major cultural shift - the current approach of communication and training are not enough if employees are left with contradictory objectives or have rewards directly linked to success indicators that do not integrate risk performance. As an example, in some financial institutions, incentives for mortgage lenders was strictly tied to the quantity of loans granted with little reference to the quality, which is what led to the 2008 financial crash.

Board Governance

Organizations' Boards need to drive ERM from the top down. Effective risk management requires:

- analysis of existing corporate impediments to effective risk management
- a structured cultural shift
- developing policies and frameworks.
- crafting procedures
- building risk dashboards
- designing control systems

Unfortunately, it often stalls at this initiation point. ERM is often treated a one-time project, while in reality it should be adopted as an on-going business process.

This article is reproduced from the November 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.

When Disaster Strikes for Off-site Employees

By Guy Robertson

Employees can work anywhere - from home, from a small branch office, from a hotel room or from a client site. If disaster strikes when they're at their regular office, they'll find the right supplies in the emergency cabinet. Emergency management people will take control and tell them what to do. When they work remotely, it's a different story. Here are the ABC's of being prepared as a remote worker

While you don't expect anything to happen while your employees are working away from the office, what should you if something happens? You can't assume that 'somebody' will look after them.

What Do You Need?

In priority order, employees who have been caught in a disaster need::

- Instructions
- First aid
- Warmth
- Water
- Food
- Communications

What Can Go Wrong?

Water — While we assume that water will be potable under most circumstances, floods and earthquakes can disrupt water management and distribution across large regions. Sewage can contaminate drinking water, and cause a number of diseases including cholera.

Dust—Dust from collapsed structures and fumes and smoke from quake-related fires can drive the need for dust masks, even gas masks.

Power—Power outages are to be expected.

Evacuation—Hotels and office buildings may be evacuated, forcing occupants to find other shelter.

Communications—Cellular phone networks are especially vulnerable to high winds, winter storms and earthquakes. They can shut down service for days. Even a big sporting event can jam phone lines. Network capacity is increasing, but so is use, and human nature can't resist the temptation to pick up the phone when an unusual event (good or bad) occurs.

What Everyone Needs When Working Away From the Office

- An electronic copy, preferably on a smartphone, of 'what to do'
- A paper copy of 'what to do'
- Appropriate clothing in case of heat loss or evacuation from hotel
- Concentrated food, often bars, ideally for at least three days
- Water purification tablets with bottle (or water) for at least three days
- A power charging source for cell phone / laptop
- Flashlight with spare batteries or crank
- Multi-tool (knife, screwdriver, file, etc.)
- Personalized first aid kit including:
  - Personal medications
  - scissors
  - whistle
  - Dust masks
  - Mylar blanket

This article is reproduced from the November 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.