TMC's ADVISOR

Covering IT and Telecom from a Canadian Viewpoint — *February 2018 , Volume 5 Issue 1*

FirstNet: National Public Safety *By Peter Aggus*

On top of the horror of the event, 9/11 was a communications disaster. When the first plane struck, emergency services personnel flooded into New York with their fire trucks, police cars and ambulances. Unfortunately, the primary way that the out-of-towners could communicate was by shouting at each other. Their radios relied on radio frequencies that didn't work in Manhattan. Similar examples abound, including the Pine Lake tornado in Alberta for which we conducted the evaluation. Since this is a common story, and communications disasters can happen at any time, FirstNet was created. It's a US story, but how long will it be until the pressure builds for Canada to follow suit?

Electronic Records Fiasco: What Now?

By Guy Robertson

You expected your new electronic records management (ERM) system to work well. The marketing literature promised efficiency, security, and convenience. Your employees were enthusiastic when you announced plans for the new system. Implementation went well - the test data was filed properly and could be found easily. Then departments began to use it for their everyday work, and problems began to arise. So what went wrong? How do you fix it now that everyone hates it?

The Death of Moore's Law and Other Big Trends

By Ellen Koskinen-Dodgson

Global spend on digital transformation technologies in 2017 was forecast at $1.2 trillion (*IDC per TechTarget*) with annual growth at 18%. While it sounds like a nice problem to have, CIOs are faced with the problem of how to spend their new money. If they choose well, they could help their company win the business disruptor game. The risk of choosing poorly can cause them to delay their decisions. Here are five big trends that need consideration when making these decisions.

C-Suite Cyber Risk Perception *By Lee-Ann Dittrich*

5th Biggest Risk

This month, Marsh-Microsoft published their Global Cyber Risk Perception Survey with responses from 1,300 senior executives with more than half at the C-suite or board level. They all agree that cyber-attacks are a serious risk, particularly because the majority of corporate value is in intangible assets such as data and intellectual property (up from 17% in 1975 to 84% now). Unfortunately, this survey shows a great deal of magical and contradictory thinking. Here's what stood out to us.

Contact Centre Assessment

Customer service has come a long way over the past few decades. Customers used to put up with a poor level of service because the bar was set low - choices were few and limiting technology and corporate policy meant that complaining didn't help. Now, customers have more choices and complaining can be much more effective. In fact, a complaint posted on Facebook or Twitter might go viral and a viral complaint can cause more damage to a company than a multi-million dollar advertising budget can repair. If you focus on making callers feel valued, you spend time to select your system and plan the configuration very carefully. You also improve your policies and procedures.

TMC can compare your reality to:

- Customer expectations
- Your own stated goals
- Your peers
- Best practices

and recommend changes so that you can meet your desired scorecard. For no-obligation information on how TMC can help you improve, contact Ellen at 604-506-2905 or ellen@tmcconsulting.ca

 ISSN 2369-663X

FirstNet: National Public Safety *By Peter Aggus*

On top of the horror of the event, 9/11 was a communications disaster. When the first plane struck, emergency services personnel flooded into New York with their fire trucks, police cars and ambulances. Unfortunately, the primary way that the out-of-towners could communicate was by shouting at each other. Their radios relied on radio frequencies that didn't work in Manhattan. Similar examples abound, including the Pine Lake tornado in Alberta for which we conducted the evaluation. Since this is a common story, and communications disasters can happen at any time, FirstNet was created. It's a US story, but how long will it be until the pressure builds for Canada to follow suit?

From 10,000 to 1

FirstNet is an independent authority within the U.S. Department of Commerce, authorized in 2012, following 9/11. Its mission was to develop, build and operate a nationwide, broadband radio network for First Responders. It would replace over 10,000 separate systems currently in use across the country.

Current Technology

Historically and currently, Emergency Services use dedicated radio systems to allow personnel to talk to each other and to their dispatchers. Each jurisdiction has its own self-contained network using radio frequencies for which they hold the licences.

City systems tend to use higher frequencies and more closely spaced towers when compared to rural systems that need to cover vast areas.

The FirstNet Approach

Rather than choosing the most fully featured technology and rolling it out everywhere, FirstNet acknowledged that they could get buy in from

emergency services in cities but no one would accept the costs of implementing this in rural low density areas.

All US states have now signed on to the proposed network that is to be provided by AT&T. FirstNet has allocated emergency responder frequencies to AT&T. AT&T will add these frequencies to their existing GSM/LTE networks and reserve them for use on FirstNet phones.

This works well in cities but not in rural areas so they chose an alternate approach for low density rural areas.

The network design includes new rural base stations to provide enhanced back-country coverage. Rural areas will have no dedicated FirstNet channels. A FirstNet phone will use the public system but will be given priority, so if no channels are available, an existing non-emergency call will be terminated and the FirstNet call will be placed.

FirstNet users can adopt reprogrammed 'normal' terminal technology supporting voice, push-to-talk, data devices, mobile hotpots etc. Some new ruggedized hardware may need to be developed.

Application in Canada

FirstNet service extends into Canada to allow US First Responders to provide assistance across the border.

It is unclear yet whether Canada will adopt a similar approach with its emergency service communications, especially since we have several jurisdictions that have recently adopted new technology bringing similar benefits. However none has so far adopted public/private partnership arrangements like FirstNet.

This article is reproduced from the February 2018 edition of ***TMC's Advisor***

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

Electronic Records Fiasco: What Now?

By Guy Robertson

You expected your new electronic records management (ERM) system to work well. The marketing literature promised efficiency, security, and convenience. Your employees were enthusiastic when you announced plans for the new system. Implementation went well - the test data was filed properly and could be found easily. Then departments began to use it for their everyday work, and problems began to arise. So what went wrong? How do you fix it now that everyone hates it?

It Started Well

The vendor's project manager helped everything go smoothly. You were very happy that it took less of your time than you expected. The vendor gave you forms to complete about 'metadata' but didn't complain when you asked that they make those decisions based on their experience.

User departments were trained on how to enter and search for data and most started entering data immediately.

Cruel Reality

Then one of your managers reported that her department had uploaded a substantial series of vital records into the ERM system, and they had vanished. To make matters worse, the department had sent the original paper records to a recycler.

An ERM consulting firm was brought in and their initial finding were:

- ERM system documentation did not cover correct procedures for your organization
- ERM orientation and training did not fully prepare system users. They entered data with the wrong coding. The data was in the system but could not be retrieved.
- Data went missing
- Searches proved difficult
- Employees made up metadata just before they loaded records onto the system

Metadata is Key

Meta is a prefix that means 'definition' or 'description'. Metadata is required for search and retrieval, to organize multi-part documents and to manage a resource, identifying when and how it was created, file type and other technical information, as well as who can access it.

Properly developed metadata are essential components of any ERM system and should be complete before the implementation.

What Now?

Once you have a fiasco, you need to step back to the design and planning stage, then roll forward properly, like a phoenix rising from the ashes. You also need to regain employee confidence.

First, what do employees need the system to do? This includes system function and metadata to search for and find documents. Is your records management policy adequate including backup procedures for records in all formats?

Re-instill Confidence

Ask employees about their experience. Was the ERM system orientation and training adequate? Did they know what to expect after implementation? Let them provide input on the best way forward as a way to win back their confidence.

This article is reproduced from the February 2018 edition of ***TMC's Advisor***

Guy Robertson is a senior planner at TMC and an instructor at the Justice Institute of BC and Langara College. He has written five 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 Death of Moore's Law and Other Big Trends

By Ellen Koskinen-Dodgson

Global spend on digital transformation technologies in 2017 was forecast at $1.2 trillion (*IDC per TechTarget*) with annual growth at 18%. While it sounds like a nice problem to have, CIOs are faced with the problem of how to spend their new money. If they choose well, they could help their company win the business disruptor game. The risk of choosing poorly can cause them to delay their decisions. Here are five big trends that need consideration when making these decisions.

Moore's Law

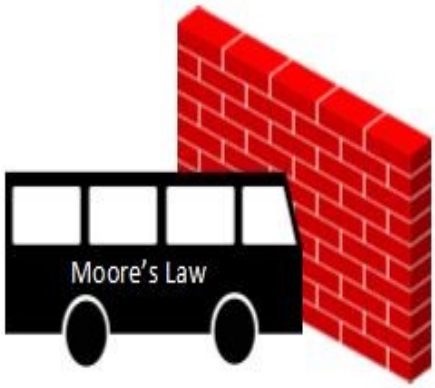
Moore's Law is named after Intel cofounder Gordon Moore. In 1965 he noted that transistors could be made smaller so that they could fit twice as many onto a chip and keep up this doubling every year. He adjusted this in 1975 to doubling every two years.

Moore's Law has driven semiconductor design improvements for fifty years and provided us with mobile phone apps, self-driving cars, Big Data analytics, and so much more. Of course, there are physical limits as transistors approach the size of atoms, and the costs of increasing miniaturization now comes with significantly increasing manufacturing cost. This means that IT hardware costs will increase over the coming years.

Skills Shortage

The IT skills shortage has been discussed for years but the major effects have not really been seen yet.

We're seeing clients using contractors to fill key positions and many have experimented with some level of contracting out. Smaller organizations or those in smaller cities are particularly vulnerable. This means



that IT staffing costs will increase over the coming years.

Multi-Cloud

Different groups within an organization have differing needs and will choose different cloud providers to meet those needs. This won't change and in fact, IT is often not consulted on the selection of a cloud provider. They may not even be aware of departmental cloud usage. IT needs to include multi-cloud into their IT Strategy, Security Plan and policies.

IoT

The Internet of Things has many business and industrial applications but the primary impetus for change within your organization will be consumer driven. Consumer device capabilities will drive user expectations of how they connect to and receive service from every business that they deal with in all areas of their life.

Employees will become attached to their consumer devices and this will drive expectations for workplace transformation, similar to what happened with the introduction of the iPhone.

Machine Learning

Artificial Intelligence has given us self-driving cars, facial recognition on facebook, and machine learning, where algorithms examine data, 'learn' from it, and make decisions or predictions. In its most elegant sense, it enables computers to find hidden insights without being told how to do so. These are largely uncharted waters so education is key here.

More Depth

We will be discussing the implications of each of these big trends in more detail in future issues.

This article is reproduced from the February 2018 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.

C-Suite Cyber Risk Perception *By Lee-Ann Dittrich*

This month, Marsh-Microsoft published their Global Cyber Risk Perception Survey with responses from 1,300 senior executives with more than half at the C-suite or board level. They all agree that cyber-attacks are a serious risk, particularly because the majority of corporate value is in intangible assets such as data and intellectual property (up from 17% in 1975 to 84% now). Unfortunately, this survey shows a great deal of magical and contradictory thinking. Here's what stood out to us.

Two Out of Top 5

The general concern about cybersecurity was reflected in the World Economic Forum's 2018 Global Risks Report, which places cyber-attacks and massive data fraud among the year's top five risks — the first time two technological risks have been in the top five. Nearly two-thirds of the Global Cyber Risk Perception Survey respondents said that cyber risk is among their organization's top five risk management priorities.

Decision Maker Disconnect

In spite of the agreed seriousness of cyber risk, 70% of respondents pointed to their IT department as their primary cyber risk owner and decision-maker.

While Boards are increasing their involvement in cyber risk decision-making (30% - 40% of respondents), they seem to be taking a head in the sand approach.

The survey reported that while 50% of Board members are provided cyber risk reports, only 18% of board members said they receive such information.

Magical Thinking

Less than 20% of respondents said that their organization has been a victim of a successful cyber-attack within the past 12 months. The survey contrasts this to a recent study by Kroll, where 85% of executives reported at least one cyber incident in the previous 12 months.

5th Biggest Risk

The conventional view was that cyber risk was a technology concern, and as a result, most organizations relied primarily on IT staff to address threats, with prevention of attacks as the driving goal.

Only 30% of respondents said that they have developed a cyber incident response plan. Such a plan defines the protocols and processes that they would follow in the event of a cyber-attack.

Respondents cited a number of reasons for not having a plan, including a belief that their organizations' defenses were adequate, reflecting conventional overconfidence that attacks can be prevented.

Respondents who did not have a plan cited a range of responses, from most common to least common:

1. Existing cybersecurity /firewalls are adequate for preventing cyber breaches.
2. Cyber incidents are covered in other crisis plans.
3. Organization lacks the expertise.
4. Not an organizational priority.
5. Cyber risk is too small to justify a plan.

Action

It is clear that IT management needs to increase their efforts to educate their Board members, perhaps providing graphic examples of the corporate harm that could occur at any time. Otherwise the "I'm sure we're OK" attitude will lead to disaster.

This article is reproduced from the February 2018 edition of *TMC's Advisor*

Lee-Ann is a researcher and business analyst that oversees benchmarking studies.