TMC's ADVISOR

Covering IT and Telecom from a Canadian Viewpoint *September 2018 , Volume 5 Issue 7*

Office Tech Lags *By Ellen Koskinen-Dodgson*

In our lifetimes we have experienced periods where our technology at home is much better than our technology that we depend on at work. This happened when 'fancy' telephones became available and when smart phones hit the market. The home/work divide is now much, much bigger than it has ever been - many people have a home filled with IoT and AI while they plod along at work with the technology of yesteryear.

The End Of The PSTN *By Peter Aggus*

Telephone service dates back to the late 1800s and has, for most of that time, been provided by copper pair cabling connecting subscribers to 'central offices' where 'exchanges' cross connect the circuits to set up calls. In its fully analog form, this is what we know as the Public Switched Telephone Network—and it is approaching the end of its life. We look at what this means for subscribers and other service providers and also what comes next.

Contact Centre Assessment

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. Does your customer service reality match your expectation? TMC can benchmark you against:

- Customer expectations
- Your peers
- Best practices

For a complimentary 15 minute discovery call, contact Ellen at ellen@tmcconsulting.ca.

Mobile Security Fail *By Lee-Ann Dittrich*

Do you sacrifice mobile security because you don't have time or don't want the hassle? If so, you're not alone. In Verizon's Mobile Security Index 2018, they identify that only 14% of companies have implemented four basic security precautions. This occurs at the same time as 93% of respondents agree that mobile devices present a serious and growing threat. Here are the highlights.

Saving Too Much *By Guy Robertson*

The tendency to save everything leads to chaos and file rooms crammed to the ceiling with useless paper. Bad records management begins with unclear policies and ineffective procedures. Without retention schedules that support your operations and allow you to discard obsolete or unnecessary records, your organization will accumulate more and more rubbish in storage areas and on corporate servers.

 ISSN 2369-663X

Office Tech Lags *By Ellen Koskinen-Dodgson*

In our lifetimes we have experienced periods where our technology at home is much better than our technology that we depend on at work. This happened when 'fancy' telephones became available and when smart phones hit the market. The home/work divide is now much, much bigger than it has ever been - many people have a home filled with IoT and AI while they plod along at work with the technology of yesteryear.

Home Tech Nirvana

Those who love their tech have tech nirvana homes. Even 'normal' people have homes loaded with tech. Why buy dad a tie for fathers day when tech is so much more fun and not that expensive?

At home, you have a virtual assistant to wake you up, tell you the weather (what to wear), tell you what time to leave based on traffic, and fill you in on the type of news that you like.

You may use augmented reality to help you multitask.

You have home security to activate a live feed on your phone when someone approaches your front door (or any perimeter) and you can talk to them before you open the door. You may even have other cameras and speakers so that you can find and call your son to dinner.

You have home automation to modify the colour of your lights by time of day to wake you up and help you get ready for sleep. The heat goes up and down and the blinds open and close as you wish.

When you leave the house, lights, TV and appliances automatically turn off

to save power and keep your house from burning down. Doors are locked and alarms are activated.

Then you get to work.

It's Like the Dark Ages

By contrast, your workplace is still in the dark ages. Someone has propped the door open because they need to unload and they forgot their door pass at home.

In reception, there's no receptionist (budget reasons), just a sign-in sheet, a phone and a list of numbers to call for your visitor to gain access. The heat is never balanced so some areas are too cold, where others are too hot.

You need information from a colleague but the best that you can do is to try to call them, then leave an email asking for a meeting. And then you work on something else while you're waiting.

Your boss says that you have 'unified communications' technology to improve productivity but it sure seems like old-school UC to you. You're not even a Millennial—the tech gap is just so obvious.

Disruptive Technology

As home tech becomes standard, the pressure to get out of the stone age at work will increase. New technologies have always been difficult to justify, yet the tipping point will come and demands for AI, augmented reality, presence, video (where's Fred?), collaboration systems and climate control to optimize productivity will increase.

How to Prepare?

Find some home-tech enthusiasts and task them with setting up a few experiments in the office to try to solve some of your productivity irritation points.

This article is reproduced from the September 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.

The End Of The PSTN *By Peter Aggus*

Telephone service dates back to the late 1800s and has, for most of that time, been provided by copper pair cabling connecting subscribers to 'central offices' where 'exchanges' cross connect the circuits to set up calls. In its fully analog form, this is what we know as the Public Switched Telephone Network—and it is approaching the end of its life. We look at what this means for subscribers and other service providers and also what comes next.

POTS

The Plain Old Telephone Service, or the ability to connect two phones, whether mobile, landline or Voice over IP (VoIP) is a service that is still much in demand even in an era of instant messaging, e-mail and video calling. However the network over which POTS is provided has been evolving since the 1990s.

PSTN

The sole carrier network for POTS used to be the familiar pair of copper wires connecting subscribers to their serving Central Office (CO). With the advent of competition in many countries, other Licensed Operators were permitted to lease PSTN local loops from the legacy Telco and put their own equipment in the CO alongside the exchanges operated by the Telco. In this way the PSTN infrastructure supported multiple service providers, many offering competing POTS services and others offering data, alarm, video, CATV etc.

As demand for capacity increased, the legacy Telcos started to replace the connections between the COs and the first cross-connection point (or 'cabinet') with fibre and this in turn drove high speed data closer to the customer. Some copper pairs were

retained to support legacy PSTN type applications but most POTS along with data and video was provided from these kerbside cabinets.

VoIP

As soon as cable TV and other operators began to compete by providing broadband IP services over CATV co-ax there was a 'new kid on the block' for providing POTS. These providers could use VoIP from the subscriber terminal, where a standard phone jack allowed users to connect a normal analog phone, back to their interconnect point.

Optical Broadband

Recent cost reductions and marketing pressures have introduced fibre connections from the cabinets to user premises—finally replacing the copper loop that defined the PSTN. Mainstream telcos around the world have now declared that they no longer regard the copper loop as their standard service and that new installations will be exclusively fibre.

The Future

POTS will still survive using VoIP technology over broadband but copper loops will disappear. Users will have a standard RJ11 phone jack on their internet router—whether provided by a cable company or a telco.

Service providers who use copper loop signalling systems, like older alarm technology or short haul data modems, will find they can no longer provide new service this way. They will have to migrate to IP networking on the back of the carrier broadband networks that are the way of the future.

Customers benefit with faster data but legacy service providers had better be ready to evolve or die.

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

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

Mobile Security Fail *By Lee-Ann Dittrich*

Do you sacrifice mobile security because you don't have time or don't want the hassle? If so, you're not alone. In Verizon's Mobile Security Index 2018, they identify that only 14% of companies have implemented four basic security precautions. This occurs at the same time as 93% of respondents agree that mobile devices present a serious and growing threat. Here are the highlights.

Basic Types of Threats

- **Denial of Service**: Jamming of wireless communications, drowning a network (or device) with fake traffic, loss or theft of a device, and ransomware
- **Geolocation**: Gathering data on location to identify the location of corporate staff in a city of interest (corporate espionage) or for data analytics
- **Information Disclosure**: Data in transit is intercepted (non-secure connections), user, app or corporate data is obtained through accessing the corporate network as a 'trusted user', eavesdropping on a voice call, secretly activating the phones microphone or camera to eavesdrop on a corporate meeting
- **Spoofing**: Email or text messages pretending to be from a legitimate corporate origin, a fake WiFi or cell base-station (Stinger, for example) which intercepts all information
- **Tampering**: Modifying data in transit, replacing a phone with a tampered device, inserting illicit software on a phone, tampering with a legitimate app, jailbreaking (Apple) or rooting (Android) a phone to bypass security

Basic Precautions

The majority of breaches are caused by not following basic security practices:

- Less than 40% change all default passwords
- Less than 40% use strong, two factor authentication on their mobile devices
- Less than 50% have a policy on the use of public WiFi
- Less than 50% encrypt data across public networks
- Only 59% restrict which apps employees can download from the internet

Where Are the Threats?

- 79% of organizations are concerned about risks from their own employees (see below)
- 73% are concerned about risks from criminals
- 72% are concerned about risks from hacktivists.
- 57% are concerned about risks from state sponsored action
- 58% are concerned about risks from their business partners

Employee Risks

Employees may:

- lose their devices
- make careless errors such as accessing corporate resources over insecure networks
- download unapproved apps
- Use weak or known passwords
- Not set up a lock-screen
- circumvent security policies
- intentionally violate security for financial or personal gain (58%)

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

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

Saving Too Much By Guy Robertson

The tendency to save everything leads to chaos and file rooms crammed to the ceiling with useless paper. Bad records management begins with unclear policies and ineffective procedures. Without retention schedules that support your operations and allow you to discard obsolete or unnecessary records, your organization will accumulate more and more rubbish in storage areas and on corporate servers.

Off Site Storage

Many organizations make the mistake of storing increasing amounts of paper off-site. Once those stuffed document boxes are out of sight, they're out of mind. The exorbitant monthly invoices for off-site storage are explained away as "part of the organizational information flow" and "the cost of doing business".

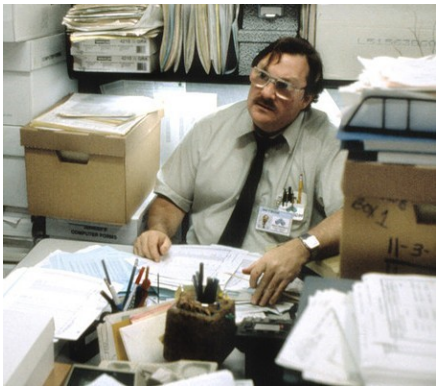
Endless Emails etc.

As for the countless useless e-mails that you and your employees neglect to delete, they're safely forgotten somewhere in the corporate network, or in the Cloud, or on somebody's laptop, aren't they? But try to find one vitally important e-mail among the enormous number on your network. Remember the proverbial needle in a haystack?

The Solution

To avoid collecting unnecessary information in any medium, consider implementing these tools:

- Manage your records from their creation to their final disposition with a well-organized records management system. This system should include proper design, use, and storage of corporate forms.



- Develop retention schedules that describe record types in all media, the length of time that you should retain them, and your method of disposing of them—shredding, secure recycling, etc.
- Use a records classification scheme that allows you to search for records in a paper file system, or in a digital records system. Your classification scheme should be clear, concise, and consistent.

The Practicalities

- A corporate leader demonstrates the advantages of using a good records management system. A lack of leadership in this area can lead to poor morale, higher costs, and higher staff turnover.
- Maximize the likelihood that employees will manage corporate records efficiently through orientation and training. No matter how good your records management system, a lack of buy-in by staff can lead to as much as chaos as if you had no system at all.
- Periodically auditing can identify the risks of your current processes and identify what should be improved.
- Disaster planning protects your records from threats such as fire, flooding, vandalism, and hostile intrusions. If a record is worth creating, it's worth saving from various forms of loss.

The Reality

Records management is easy to neglect. In many cases a wake-up call comes when an organization is cited for non-compliance with the Fire Code or with Access to Information requirements.

This article is reproduced from the September 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.