The TMC ADVISOR

The Advisor is a periodical published by TMC containing articles of interest to Canadian Business Professionals *Aug 2021, Vol 8 # 4*

Non-collaborative Collaboration *By Peter Aggus*

Companies choose a platform for video/web conferencing, instant messaging, telephony, voicemail, file sharing etc., and it works well for all corporate users. Unfortunately, the internal collaboration system doesn't inter-work well with outside participants' internal or cloud systems. Everyone needs to download apps for Zoom, Teams, etc. so that they can join someone else's meeting. Things look to be changing with developments in gateways.

Build a Virtual Go-Bag *By Ellen Koskinen-Dodgson*

In this time of wildfire evacuations, people in risk areas are advised to keep a personal 'Go-Bag' handy in case they need to drop everything and go. Evacuations can happen at work, too, triggered by a wildfire, a gas leak, or for other reasons. If you need to evacuate, we recommend that you prepare a virtual Go-Bag with priority items you need to recover your business operations. Here's what should be in it.

How Do You Rate?

Our IT Assessment Team can identify and explain how you compare to best practices on:

- Reliability
- Staffing Levels
- Costs
- Customer Service

For a free copy of "What to Assess and Why," email: assessment@tmcconsulting.ca.

Cloud Security Roundup *By Maria Colasurdo*

Cloud security risks are a big concern and are getting worse, according to four recent studies. As examples, 97% of Google Workspace users have authorized at least one third-party app to have access to their corporate Google account and 89% of organizations say that microservices, containers, and Kubernetes have created application security blind spots. Here's a high-level review.

Audit Your Own BCP/BRP *By Guy Robertson*

You've been working from home for the past 18 months, and a lot has changed - including your office's risk profile. If you're like many others, your business resumption plan (BRP or BCP) lives in an "out of sight, out of mind" state, perhaps sitting in binders gathering dust on the shelf or buried in SharePoint or in a corner of a website. It's time to blow off the dust and audit it. Here's how to do that yourself.

ISSN 2369-663X21

Non-collaborative Collaboration *By Peter Aggus*

Companies choose a platform for video/web conferencing, instant messaging, telephony, voicemail, file sharing etc., and it works well for all corporate users. Unfortunately, the internal collaboration system doesn't inter-work well with outside participants' internal or cloud systems. Everyone needs to download apps for Zoom, Teams, etc. so that they can join someone else's meeting. Things look to be changing with developments in gateways.

How We Collaborate

Collaboration is 'the process of two or more people, entities or organizations working together to complete a task or achieve a goal'. It encompasses a variety of media.

Historically, most collaboration was in-person (meetings, conferences, etc.) and by telephone. Material was transmitted by physical delivery or electronically (fax, telex, etc.).

These days, material is usually sent electronically by e-mail, although fax and file transfer sites like Sync are also used because of their security advantages. Telephone calling has evolved to include voicemail, IVR, speech recognition, video/web, chat and mobile integration. Stand-alone video conferencing systems were developed to fill a business niche before the development of video/web conferencing .

Voice Is Still Prime

In the over 40 age group, phone and e-mail are the preferred media, while under 40s like phone and web/mobile messaging and chat. Clearly the phone is still the main, if slowly declining, medium—60% of >65s falling to 42% of <25s rate it as their preferred medium.

Voice has been the foundation of remote collaboration and many organizations continue to operate a

private in-house voice system as it has lots of life left in it. Over the years these voice systems have been upgraded to include ever more integrated collaboration functionality.

Internal vs. External

While internal voice-based systems had developed a full suite of collaboration capabilities, they continued to have a major shortcoming. If you want to run a video/web conference call you would have difficulty integrating participants outside your organization.

The pandemic drove the need for anyone-to-anyone collaboration and many employees suddenly became 'outsiders' as they stayed home and tried to do their jobs. The in-house voice-based collaboration system could not quickly and economically be expanded to fill the need.

External providers like Zoom offered an easy solution and suddenly 'everyone' was using Zoom. Microsoft Teams and Cisco WebEx remain major players in the corporate and government space. For example, Microsoft Teams is used by 9 out of 10 Fortune 100 companies.

Gateways

There is no collaboration product, on-premises or cloud-based, that solves all organizational collaboration issues:

- Retention of existing systems
- Cost
- Security
- Functionality
- Support for remote users
- Inter-working with 3rd party collaboration systems
- Inter-working with 3rd party CRM and other applications

Gateways or gateway services seem to be the emerging solution. Phone systems suppliers like Avaya, Cisco, Mitel, NEC, etc. have developed integration with Microsoft Teams and Google G Suite, Salesforce.com, etc. Expect ongoing developments in gateway functionalities.

If you'd like to comment on this article or explore these ideas further, contact me at peter@tmcconsulting.ca.

This article is reproduced from the Aug 2021 edition of ***The TMC Advisor***

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

Build A Virtual Go-Bag *By Ellen Koskinen-Dodgson*

In this time of wildfire evacuations, people in risk areas are advised to keep a personal 'Go-Bag' handy in case they need to drop everything and go. Evacuations can happen at work, too, triggered by a wildfire, a gas leak, or for other reasons. If you need to evacuate, we recommend that you prepare a virtual Go-Bag with priority items you need to recover your business operations. Here's what should be in it.

Virtual Is Best

Life safety is critical above all else so a physical go-bag might not work for you. When the day comes, you might not have a chance to collect it and carry it out with you. You might not even have a chance to grab your wallet or car keys as you make a run for it.

A 'virtual go-bag' means that you have arranged all priority items you'll need to be off-site, secure and ready to use. To the question of physical vs. cloud, either will work if they keep your data outside of your evacuation zone and it contains what you need to resume business operations—at least the most critical operations.

Ideally, this should include good backups, transaction logs, digital versions of work-in-progress, and of critical importance: instructions of what to do. Just think - if Fred and Susan know how to restore service, what will you do if neither is available due to vacation or sick leave?

Backups

Basic backup processes allow you to recover your business data as of the moment you did that backup. However, if you only back up weekly, then your business could lose a week of data. Even daily backups can leave a gap.

Logs

Transaction logs record every action for all mission critical applications. Restoration is now a case of reloading the backup and then reloading the log to get up to date. If you have a remote disaster recovery site on your network copy logs there. If not, then use a cloud service and keep it in sync with your main operation.

Paper

You really need to think about the flow of all information around your business in all forms, including work-in-progress – think in-trays and papers on desks.

Ideally you will design your business processes to secure critical data as soon as possible, likely by scanning important paper documents.

Recommendations

Look at your business processes and information flow. Identify which information is vital for business resumption and whether it's protected through backups and logs.

Review your paper work-in-progress handling. Does it remain in paper form until a transaction is completed in the appropriate business application or do you scan it so that it can be stored in digital form as a precaution should you need to evacuate the building before the transaction is completed?

Check your recovery point objectives. If they were established years ago, decide if they need to be updated.

If your RPO is for 4 hours and your backup, log schedules and work-in-progress digitization schedules don't support this, you have work to do.

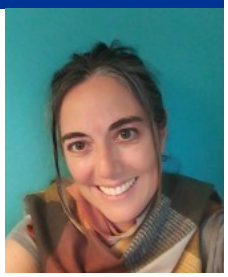
Make sure your backups, logs, and work-in-progress digitization are off site and secure.

If you'd like to comment on this article or explore these ideas further, contact me at ellen@tmcconsulting.ca.

This article is reproduced from the Aug 2021 edition of ***The TMC 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 Security Roundup *By Maria Colasurdo*



Cloud security risks are a big concern and are getting worse, according to four recent studies. As examples, 97% of Google Workspace users have authorized at least one third-party app to have access to their corporate Google account and 89% of organizations say that microservices, containers, and Kubernetes have created application security blind spots. Here's a high-level review.

Security Pros

Cisco published a 2020 survey of 4800 security professionals asking which security practices had the biggest impact on business outcomes. They found that:

- If you want to achieve overall program success, including retention of security talent, devote resources to proactive tech refresh and integrate your technology.
- If you want a strong security culture that's embraced by all, focus on good equipment, clear direction, accurate alerts, and timely fixes of security issues.

CISO's

Dynatrace commissioned Coleman Parkes to conduct their 2021 Global CISO report which included input from 700 CISOs of large (>1000 employee) companies. Their findings included:

- 77% say most security alerts and vulnerabilities are false positives that don't require actioning as they're not actual exposures
- 67% say the volume of alerts makes it very difficult to prioritize vulnerabilities based on risk and impact
- 57% say alerts lack information needed to ensure the most critical vulnerabilities are fixed first.

AWS Security Pros

The Cybersecurity Insiders 2021 AWS Cloud Security Report surveyed 300 security professionals to find that:

- 95% of cybersecurity professionals confirm they are extremely to moderately concerned about public cloud security.
- The top 3 concerns include Misconfiguration of the cloud platform (71%), Exfiltration of sensitive data and Insecure APIs (54%).
- >40% of organizations embrace hybrid cloud (44%) and multi-cloud deployments (43%) for planned redundancy because of commitments to legacy applications in traditional data centers. Single cloud deployments (11%) continue to diminish in importance.
- 90% of organizations use more than two cloud providers.

Executives

In their 2021 study of 4300 executives, they found that tech Leaders, the top 10% of the survey group, were growing company revenues at 5x the speed of tech Laggards, the bottom 25% of the group. The study also saw 18% of the survey group emerge as Leapfroggers, who grew at 4x the rate of the Laggards.

The Leaders, and now the Leapfroggers, demonstrate three strategies that underlie their success:

1. They move to and innovate in the cloud.
2. They reframe, adopting innovation -led strategies.
3. They flip their IT budget allocation to favour innovation from a traditional 70/30 split for maintenance/innovation and new spending, to a 30/70 split, keeping the IT budget unchanged.

If you'd like to comment on this article or explore these ideas further, contact me at maria@tmcconsulting.ca.

This article is reproduced from the Aug 2021 edition of *The TMC Advisor*

Maria is a skilled researcher and oversees TMC benchmarking studies.

Audit Your Own BCP/BRP *By Guy Robertson*

You've been working from home for the past 18 months, and a lot has changed - including your office's risk profile. If you're like many others, your business resumption plan (BRP or BCP) lives in an "out of sight, out of mind" state, perhaps sitting in binders gathering dust on the shelf or buried in SharePoint or in a corner of a website. It's time to blow off the dust and audit it. Here's how to do that yourself.

Planning Materials

Review your disaster planning materials to identify out-of-date, incorrect or incomplete information:

- risk assessments and analyses
- mitigation measures
- personal safety procedures
- data back-up and recovery processes
- security technology (building access, etc.)
- strategic alliances
- orientation and training
- emergency supplies and equipment.

Discuss your current plan with department representatives and request their ideas for updating of the plan and adding new material.

Pay particular attention to the ways in which pandemic management and wildfire problems have been addressed. Just because your office is in an urban area you are not necessarily protected from wildfires. They can occur in a tree-lined median or nearby park.

Compliance

Review the list of your office's compliance requirements. These might include federal, provincial and

municipal government legislation, guidelines, and regulations. These regulations will include your regional and local Fire, Building, Safety and Emergency Management Codes, industry-specific regulations, and may include PCI and ISO standards for credit card processing and IT security.

Privacy

Review the list of your office's privacy requirements. This would include provincial and federal legislation. Consider the implications of insufficient information security and unsuitable storage. Make sure that you have completed privacy impact assessments (PIAs) for your computer applications.

Head Office

Look for contradictions between your office's disaster plan and that of your head office; confirm that any discrepancies are warranted.

Identify opportunities to derive useful information from your head office's disaster planning materials.

Identify opportunities to cooperate with head office in the development and delivery of orientation and training programs.

The Final Step

When you have updated your BRP, set a date for testing it with a tabletop exercise. Convene in a meeting room or in your Emergency Operations Centre with or without a test facilitator. Attendees will open an envelope explaining the disaster with instructions of how they need to use your BRP to resume operations.

By the end of the exercise they will understand where the BRP failed to help them reach their objectives. Incorporate what they've learned into your updated plan. Schedule your next exercise.

If you'd like to comment on this article or explore these ideas further, contact me at guy@tmcconsulting.ca.

This article is reproduced from the Aug 2021 edition of ***The TMC 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.