The TMC ADVISOR

The Advisor is a registered TMC publication for Canadian Business Professionals *October 2020 , Volume 7 Issue 7*

Have You Been Hacked? *By Ellen Koskinen-Dodgson*

Maybe you've completed a pen test on your network and the penetration tester was able to get in without much trouble. You've followed their advice to improve your security posture and you're feeling much better about things except…the report included the following worrisome words: "This test did not assess whether you have been hacked." Can it be true that someone has hacked you and you don't know? Of course. Here are some DIY actions that you can take.

How Old is Your Disaster Plan? *By Peter Aggus*

The aim of a Disaster Plan (DP) is to document your business systems and processes and describe how you plan to recover should an event disrupt or stop your operations. The DP needs to be a living document and should reflect today's operations, not how things used to be when it was written. As you contemplate updating your DP, here's your trip down Memory Lane about how out-of-date things could have come to be.

Fast Recovery – a Five Step Process

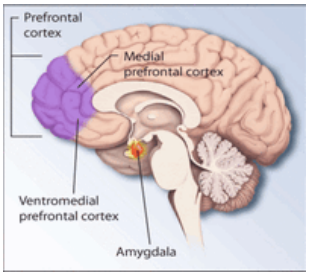
1. Assess your Disaster Recovery Plan – identify what's missing or out of date
2. Review your risks
3. Update your DRP
4. Activate mitigation plans including rearchitecting infrastructure for fastest recovery
5. Train and test

For a more extensive document, request "Fast Recovery" from ellen@tmcconsulting.ca.

Proximity Risks: What's Next Door? *By Guy Robertson*

You work very hard to identify and mitigate risks on your own premises, yet when disaster strikes, you're crippled, maybe down for the count. Look out your office window. Around or near your building, there stand structures that might be at risk for fires, floods, and gas leaks. Their events extend to you: a traffic shutdown can stop your traffic; proximity to a crime scene can shut you down. Proximity risks are a big deal and need to be addressed.

Conversational Intelligence *By Thomi Glover*



Several of my clients have said that they find it almost impossible to "read" other people on zoom or the like. Though doing business through a variety of on-line platforms is now commonplace, many of us long for face to face meetings where it is easier to "pick up the vibes" from others. Without that proximity, we feel we are at a real disadvantage in forming working partnerships. Fortunately there is another approach - "Conversational Intelligence."

ISSN 2369-663X

Have You Been Hacked? *By Ellen Koskinen-Dodgson*

Maybe you've completed a pen test on your network and the penetration tester was able to get in without much trouble. You've followed their advice to improve your security posture and you're feeling much better about things except...the report included the following worrisome words: "This test did not assess whether you have been hacked." Can it be true that someone has hacked you and you don't know? Of course. Here are some DIY actions that you can take.

Historical Logs

A good first step is to check your log files on servers, networking, and security systems. If they've been deleted, check the date that they were deleted or stopped and then restarted. Hackers like to delete logs to cover their tracks.

If your logs were not deleted, it doesn't mean that you were not hacked. Have a skilled person read your logs to identify suspicious activity.

Internet Traffic Reports

Review your internet traffic reports to look for traffic when there should be little or no activity or even unusual levels of traffic during normal traffic hours. Look back at least 6 months.

Quick Detection

Even with an effective security strategy, there's no way to guarantee that you won't get hacked. It therefore makes sense to detect intrusion as soon as possible and take quick action.

Make it your job to understand and pay attention to log files, either manually or through automated monitoring, detection, and prevention systems. This is often very difficult to do as there are so many "urgent" demands on our time.

Isolate Your Back-ups

Back up your logs and keep all of your back-ups isolated from your network, except during backup. Then if you get hacked, the hackers won't get access to your back-ups.

DR Site

DR sites are not just to get you up and running after a fire. Some organizations use their DR site to be ready to go with your top business software.

With your protected backups, you could be up and running with yesterday' back-up data in very short order after you detect an intrusion.

Set Traps

Stationx CanaryTokens is a site worth exploring. Basically, you can create files that, when opened, trigger an email that the file has been opened, and from where. See https://www.stationx.net/canarytokens/

There are various ways to use CanaryTokens. Among the many options, you could arrange to be alerted if:

- Someone opens a Word, Excel, pdf or email file that contains your trap token.
- Someone clicks on a targeted URL.

In all cases, you'll increase your hit-rate if you choose an enticing name.

Despite the many options of where and how to set traps, many intruders know how to detect common traps. Happily, there are things that you can do to make your traps more difficult to detect.

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 October 2020 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.

How Old is Your Disaster Plan? *By Peter Aggus*

The aim of a Disaster Plan (DP) is to document your business systems and processes and describe how you plan to recover should an event disrupt or stop your operations. The DP needs to be a living document and should reflect today's operations, not how things used to be when it was written. As you contemplate updating your DP, here's your trip down Memory Lane about how out-of-date things could have come to be.

Media

Years ago you might have stored your DP in binders. Perhaps you were leading edge and stored it on floppy disks as that that would make it much more useful. It was, at the time,—but how do you read that floppy now? Perhaps your DP is a little newer so it's on a CD. Will you have a CD reader when you need it?

Telecom Systems

How useful is a DP that tells staff where to find the lubricating oil for the PBX switches? The last PBX with moving parts that needed oiling has long been recycled.

Maybe your plan is newer and tells you where the PBX software is stored – on floppy disks. Maybe it's newer still but not new enough. You've long since replaced the old phone system and changed the maintenance supplier. What system do you have? Whom do you call to restart it?

Other IT Infrastructure

You probably have a modern Ethernet -based LAN—but does your DP still think the world runs on token ring, or even dial-up?

Maybe your inter-building links used to be over telco leased lines and your plan reflects that. In some

jurisdictions, leased lines don't even exist any more. The telcos pulled the copper out and sold it for a lot of money.

Perhaps you've virtualized since you last updated your plan or you might have moved away from Star Wars themed server names. Out-of-date instructions about restarting Chewbacca can read like spy code.

If your plan is old enough, it might think that you still have that old mainframe that you worshipped decades ago. Maybe it tells you where to find the boot floppy disks. Lol, floppy disks used to rule.

Contacts

Probably the biggest problem area in a DP is instructions to call staff who retired long ago or at out-of-date numbers. This is also the fastest way to obsolete any new plan. We recommend using functional job titles rather than the names of people along with links to current staff directories.

Risks and Rewards

Some organizations are surprised to find that full recovery can take a month or more and that they may not even be able to recover some of their processes. If you do things right, you can recover in less than a day, even if you've been ransom-wared.

Our consultants regularly work with clients to review their DPs and compare the content with what is currently in use. They also work together to develop fast recovery processes, often by rearchitecting the infrastructure.

A Self-Test

Dig out your Disaster Plan, check the date and start reading. Check if it has been annually tested. Start counting out-of-date information.

Because when it comes right down to it, an obsolete Disaster Plan is only funny if it applies to someone else.

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 October 2020 edition of ***TMC's Advisor***

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

Proximity Risks: What's Next Door? By Guy Robertson

You work very hard to identify and mitigate risks on your own premises, yet when disaster strikes, you're crippled, maybe down for the count. Look out your office window. Around or near your building, there stand structures that might be at risk for fires, floods, and gas leaks. Their events extend to you: a traffic shutdown can stop your traffic; proximity to a crime scene can shut you down. Proximity risks are a big deal and need to be addressed.

Beyond Your Perimeter

Your building may be safe and well-constructed in itself, but it remains vulnerable to the nearby structures and landscape features. Your organization's Risk Register needs to include proximity risks and your Risk Mitigation Plan needs to address them. Consider your building's proximity to:

Neighbouring Buildings may have:

- Inadequate fire controls
- Inattention to the requirements of the Fire Code
- Older plumbing and electrical circuitry
- Substandard maintenance
- Older structures unable to withstand earthquake loading
- Inadequate security procedures
- Inadequate sanitation
- Inadequate pest control
- Criminal activities, e.g. narcotics distribution

Roadways may experience:

- Closures following a motor vehicle accident, or a local emergency such as a fire or gas leak

- Reduced flow owing to debris, precipitation and abandoned vehicles in roadways after a storm, fire, or earthquake

Retail Shopping Areas

Proximity to shopping areas is often related to incidents of robbery, arson and vandalism.

Gas Stations and Fuel Tanks

Fuel spills, fires, and explosions can occur on any site that contains fuel tanks. In many cases the cause of these problems is human error.

Parking Lots

Parking lots are often scenes of muggings, vandalism, and assault.

Air Traffic

Buildings located near airports, and especially any location in the flight path of aircraft, could be at risk for aircraft accidents. Fortunately, such accidents are rare.

Bodies of Water

Rivers and lakes are the bodies of water commonly associated with flooding. Note, however, the risk from clogged street drains and sewer backups.

Crime Hotspots

The most common criminal risks might be vehicle theft and break-ins, mugging and assault, vandalism, shoplifting, and distribution of illicit drugs and stolen goods.

Action Plan

Find your site on Google Maps and see what kinds of risks surround you. Better yet, walk around and note those risks.

Address those risks in your Risk Register and Mitigation Plan. They're not going away. 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 October 2020 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.

Conversational Intelligence *By Thomi Glover*

Several of my clients have said that they find it almost impossible to "read" other people on zoom or the like. Though doing business through a variety of on-line platforms is now commonplace, many of us long for face to face meetings where it is easier to "pick up the vibes" from others. Without that proximity, we feel we are at a real disadvantage in forming working partnerships. Fortunately there is another approach - "Conversational Intelligence."

The Problem

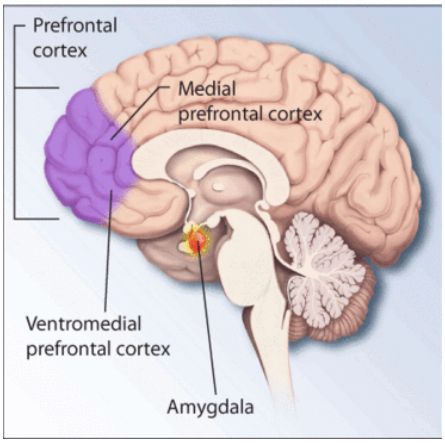
Our neanderthal ancestors' brains differed from ours in one primary respect....their limbic brains and amygdala in the back and lower part of the skull were highly sensitive. They needed to "know" when danger was close and when it was time to get away fast! They were good at that and evolved into us, homo sapiens.

Our critical difference is the development of the prefrontal cortex...that front part of the brain where our thinking and trust response resides. The problem is that the amygdala can derail our trust building capacity in a heartbeat, whenever we feel threatened in any way, be it by business uncertainty and anxiety or by mixed messages from others.

Help for Consultants

Many people have heard of emotional intelligence, that combination of skills that Daniel Goleman defined as self awareness, self management and relationship effectiveness. My coaching clients ask me, "How do I demonstrate these critical skills when I communicate and what can I do to create better partnerships with my clients?

This is where conversational intelligence comes in.



From "I" to "We"

Many people find themselves in a consulting role, either as actual consultants, like my colleagues at TMC, or by serving "internal clients" within an organization in their role as an IT Manager or as the manager of another support department.

A consultant's task is to partner with their clients, which absolutely requires shared trust and honesty. This means that they need to move from "I" (the consultant, with lots of knowledge and the personal need to be successful) to "We".

There are three common conversational blind-spots which hinder this:

1. We jump to solutions for client problems as being right provides us with a dopamine high...it can be addictive.
2. We fail to realize that when we feel anxious we release cortisol which closes down the prefrontal cortex—our thinking place. So no problem solving or decision making there.
3. We "know" what someone has said, but it's often not so. We usually recall what we were thinking about what the other person has said. Our own (and our client's) internal dialogue can block accurate communication.

We need therefore to ensure we have actually communicated with our clients; that we have actually understood one another.

In our next issue we'll review how to improve our chances of understanding and being understood.

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

This article is reproduced from the October 2020 edition of ***TMC's Advisor***

Thomi is an Executive Coach, Leadership and Organizational Development Consultant and facilitator of custom processes that build effective teams, enhance leadership and develop emotional intelligence.