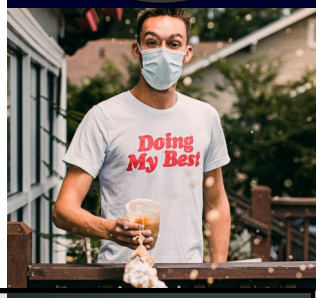
The TMC ADVISOR

The Advisor is a registered TMC publication for Canadian Business Professionals **September 2020 , Volume 7 Issue 6**

Before the Security Scan Part 2 *By Ellen Koskinen-Dodgson*

When you run vulnerability scans or pen tests, best practice is to first lay groundwork and "clean up your act," data-wise. The scan can then be a report card as well as a road map. Previously, we addressed foundational issues: creating a Security Committee, identifying critical or sensitive information and identifying the risks. Now we discuss prioritizing risks and establishing mitigation plans, as well as adopting recommendations from a scan.

Whoops! Human-Caused Risks *By Guy Robertson*



The most destructive human-caused risk to any organization is war, with civil unrest and rioting coming in as close seconds. Luckily, the most common human-caused threats are less dramatic, but in some cases, they can also cause extensive damage. Apathy, carelessness, forgetfulness, inattention, and ignorance are such widespread concerns, that it's safe to assume that every organization has suffered because of them.

What Type of IT Department Are You?

There are 3 kinds of IT departments, find out where you stand:

Run: Keeping the lights on

Grow: Improving existing systems

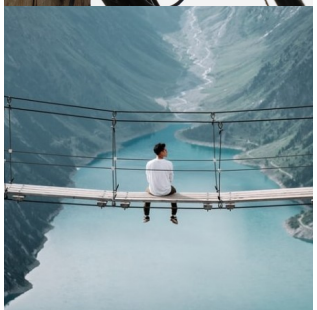
Transform: Changing the nature of the business

For more information, or to request a free copy of "IT Assessments 123,"
email: assessment@tmcconsulting.ca.

5G Update *By Peter Aggus*

We were promised lots—but, as is typical for complex developments, rollout takes time. So what is going on? Time for a closer look at what Canadians can now do with 5G and when the promised "big gains" will arrive. Should you switch to 5G now, or keep waiting? Who is offering service? Are there many 5G phones available yet? How might all of this be affected if Canada opts to join other countries and remove Huawei equipment from the networks?

Bridging the Skills Gap *By Elleni Koskinen*



The digital skills gap is an issue currently affecting organizations around the world. Even the most technologically advanced companies are coming face-to-face with the reality that the work is evolving faster than their workforce. With a lack of digital skills within their own people, and a very limited number of trained graduates emerging into the candidate pool, what are these companies to do?

ISSN 2369-663X

Before the Security Scan Part 2 *By Ellen Koskinen-Dodgson*

When you run vulnerability scans or pen tests, best practice is to first lay groundwork and "clean up your act," data-wise. The scan can then be a report card as well as a road map. Previously, we addressed foundational issues: creating a Security Committee, identifying critical or sensitive information and identifying the risks. Now we discuss prioritizing risks and establishing mitigation plans, as well as adopting recommendations from a scan.

Risk Register

Once you have identified risks to critical or sensitive information, it's time to develop an information risk register. Every organization's risk register looks somewhat different, but at a minimum, we recommend:

- **Title** (a short-hand way to name the risk, such as *Data Loss While Travelling*)
- **Source of Risk** (such as *Devices are stolen or lost*)
- **Location of At-Risk Data** (such as *Laptops, tablets and smart phones*)
- **Owner** (which senior manager is responsible for mitigating this risk, such as the CIO)
- **Existing Mitigation** (such as *Devices are password protected*)

The risk register also contains the risk assessment which is calculated on a 9 or 25 point scale. It uses three columns of the register:

- **Frequency** (how common is the risk on a 1-3 or 1-5 scale)
- **Impact** (how much harm would it cause on a 1-3 or 1-5 scale)
- **Severity** = *Frequency* x *Impact* on a 1-9 or 1-25 scale

Finally, the register includes columns for tracking the progress of an action plan, if there is one. For example, loss of

information through paper-only records could be mitigated through scanning the documents and filing them in an electronic records management system. The tracking columns of the risk register could include:

- **Open Date** (when the risk was acknowledged and the mitigation plan initiated)
- **Close Date** (if any)
- **Mitigation Plan (**such as *Encryption of sensitive information*)
- **Status** (regular updates to ensure progress)

Scanning

Vulnerability scanning vs. penetration (pen) testing—both are needed.

A vulnerability scan effectively runs through a checklist of known vulnerabilities (over 50,000) and reports how many of those problems exist on the system. Scans are run on a monthly (or more frequent) basis.

The scanner will rank vulnerabilities by level of risk. Sifting through reported vulnerabilities and making sure they are not false positives is part of the process. There are strategies to reduce the number of false positives.

Pen tests are real-time, manual tests by Ethical Hackers to test defenses and give more accurate and thorough results. Pen tests can range from a day to a week and can be expensive, depending on the extensiveness of the test. They can also affect operations by slowing processes, and interfering with staff productivity.

After the Scan

The recommended actions that affect critical and sensitive information are then logged onto your information risk register and tracked.

An important part of reducing your liability is demonstrating due diligence.

This article is reproduced from the September 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.

Whoops! Human-Caused Risks *By Guy Robertson*

The most destructive human-caused risk to any organization is war, with civil unrest and rioting coming in as close seconds. Luckily, the most common human-caused threats are less dramatic, but in some cases, they can also cause extensive damage. Apathy, carelessness, forgetfulness, inattention, and ignorance are such widespread concerns, that it's safe to assume that every organization has suffered because of them.

Humans and Tech

"One of the more challenging aspects of dealing with customers," said a retired salesperson from a large computer manufacturer, *"is to convince people that one of the biggest risks to any IT system is human carelessness. People delete enormous amounts of data accidentally. They trip over cables and disable entire departments. They leave their laptops and other portable equipment on buses, trains and planes. They leave the server room unlocked. Many of us have made these mistakes."*

The Foundation of Risks

Apathy: "I really don't feel like reviewing this data backup procedure. Boring! I'll do it next week, maybe, if I find the time."

Carelessness and Clumsiness: "Whoops! I dropped that big old binder of systems documentation that everyone makes a fuss about, and the binding broke. But I gathered up all of the loose pages, that is, except for a few in the middle. I don't know where they went. Sorry."

Forgetfulness: "I forgot to lock the server room, and now you're missing the server with all of the marketing data."

False Assumptions: "I thought that the executive assistants would bring in

those boxes from the loading bay, and they didn't. Those laptops got wet last night when it rained. There were some packages from other suppliers, too. They got really wet, but they should be fine when you dry them out, right?"

Inattention to Detail: "Did I back up all of today's financial data? Perhaps not. Well, if you lose any, that's a pity."

Ignorance of Internal Policies: "Is it okay to show visitors around the vault? Some fellow asked to see our client files, so I showed him where they were in the vault, and he seemed very grateful. He was in there for quite a while. Are you missing any of those files? No, I haven't had a chance to read the security manual, but I will, maybe next week."

Inattention to Laws and External Regulations: "One of our older employees had a heart attack in the staff room last week, and none of us knew what to do. Somebody should have administered first aid, but nobody on staff had the training, so that unfortunate employee had to wait until an ambulance arrived, and that took quite a while. Our occupational health and safety code demands that we have at least one fully trained first aid attendant on site during business hours, so I guess one of us should take the training. When? Oh, sometime soon."

The Result

Such statements seem outrageous, but they are reproduced here verbatim from sources in Canada, the US, and Britain. You must never underestimate the likelihood of human-caused risks, which most commonly result in lost data and other valuable assets, damage to fixtures and facilities, breaches of employee and client privacy, and loss of the organization's reputation.

This article is reproduced from the September 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.

5G Update *By Peter Aggus*

We were promised lots—but, as is typical for complex developments, rollout takes time. So what is going on? Time for a closer look at what Canadians can now do with 5G and when the promised "big gains" will arrive. Should you switch to 5G now, or keep waiting? Who is offering service? Are there many 5G phones available yet? How might all of this be affected if Canada opts to join other countries and remove Huawei equipment from the networks?

5G or 4G LTE or Wi-Fi?

We last wrote about 5G in September 2019. We explained then that 5G is both a new signalling protocol and a new set of radio frequencies. 5G service will be offered on the same frequencies as 4G (LTE)—called low-band. It will also be offered on frequencies similar to Wi-Fi—called mid-band. The new frequencies above 30GHz are called hi-band. There is little difference between low-band 5G and 4G LTE or mid-band 5G and Wi-Fi—aside from the signalling protocol used. We expect to see comparable speeds and bandwidth to services currently using those frequencies. The big gains expected from 5G will only come with hi-band.

Upgrading 4G LTE

This is a natural evolution of what exists and is the favoured (low risk) path for carriers. Capacity on existing LTE sites will be switched to 5G so new phones can enjoy 5G protocol. Where sites do not offer 5G, the phones will fall back to 4G. Telus, for example, has been investing heavily in higher density 4G service via eNode fibre-distributed antennae (see photo). These are active right now on 4G LTE service with hundreds deployed on utility poles in many areas of the Lower Mainland and Southern Vancouver Island. They will likely carry 5G low-band service initially,

but could be upgraded to higher frequencies later.

Linking with Wi-Fi

Shaw is quietly rolling out its own cellular service, blending their Freedom Mobile LTE service and Shaw Go Wi-Fi to offer seamless roaming and high density from their existing Wi-Fi investment. Future dual-use nodes could see those Wi-Fi hubs offering 5G mid-band service.

5G Hi-Band

Telus is offering 5G hi-band service in Vancouver, Toronto, Montreal, Calgary, and Edmonton. Bell is opening in the same cities. Rogers currently offers 5G in Vancouver, Toronto, Ottawa and Montreal. Shaw does not currently offer 5G service but expects to start soon.

Phones and Plans

Presently, the Galaxy S20, LG V60 and Motorola edge+ are the only available options for 5G phones. We are starting to see "unlimited" data plans for 5G, but be careful: that unlimited might only apply to 5G and not when falling back to 4G. 5G hi-band will offer a claimed "up to 1.7Gbps" data rate. 4G fallback will enjoy 150Mbps data rates. When 5G lo-band service is offered that should increase—up to a theoretical 1.5Gbps.

The Huawei Joker

As we saw last month in "Beware of the Dragon," countries like the US, the UK and Australia are mandating the removal of Huawei equipment from their networks. Currently Canada has not joined in, but many see it as only a matter of time. The eNode systems deployed by Telus are supplied by Huawei, but the new 5G hi-band systems are mainly sourced from Samsung, Nokia and Ericsson. Other carriers will likewise be planning to reduce reliance on Huawei for 5G—although Huawei equipment is still littered throughout the 4G networks.

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

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

Bridging the Skills Gap *By Elleni Koskinen*

The digital skills gap is an issue currently affecting organizations around the world. Even the most technologically advanced companies are coming face-to-face with the reality that the work is evolving faster than their workforce. With a lack of digital skills within their own people, and a very limited number of trained graduates emerging into the candidate pool, what are these companies to do?

Time to Train

A short-term solution to discovering a lack of skills within your workforce would be to hire specialists to fill those roles. Of course, this comes at a premium price. A long-term, more practical solution is to reskill the employees you already have. Offering in-house re-training will be critical to ensuring that your company isn't left behind as the digital era surges forwards.

Surprisingly, this isn't an unpopular opinion. The majority of hiring managers agree that digital skill development programs are vital to keeping their organizations afloat amid industry disruptions and innovations, but many have been slow off the mark. Whether a lack of budget, time, or employee motivation, many companies have found excuses rather than results. However, in order to stay relevant, these companies will need to act now, or else be surpassed by others that did.

Take Advantage of Tech

There are already several online learning platforms to help companies foster an environment of lifelong learning. Organizations should take advantage of them and develop their own program

guides to enable their employees to succeed in their field. Platforms such as Coursera, Udacity, and Udemy offer courses in data science, machine learning, and AI, and can help businesses succeed in transforming their workforces. According to the *World Economic Forum*, a company's future success may rely on their ability to "harness new and emerging technologies to reach higher levels of efficiency," which won't be possible without reskilled employees.

Be the Right Employer

Today more than ever, employees are dedicated to working for companies that they can be proud of. Organizations that value their employees, offer friendly, respectful environments, and boast strong values are the ones that retain their workers. Attracting talent or creating talent within your workforce from the ground up is only valuable if you can keep them around. Employees that have the necessary skills to fill the digital gap will have their pick of jobs, so an inflated salary and benefits package may not be incentive enough. Research shows that companies that lead with their morals, foster workplaces that value diversity and inclusivity, and create a positive social impact are the ones that will win the war for talent.

Next Steps

It should be mentioned that there are no hard and fast rules for which companies will thrive, which ones will survive, and which ones will be left by the wayside. In fact there is no one-size-fits-all answer for how to successfully future-proof your workforce. However, by upskilling, taking advantage of lifelong learning opportunities, and focusing on employee retention, organizations will be well poised as we enter the 4th industrial revolution.

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

Elleni Koskinen is the editor of the Advisor, a skilled researcher, and oversees TMC benchmarking studies.