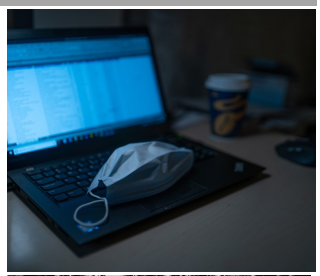
TMC's ADVISOR

Covering IT and Telecom from a Canadian Viewpoint — *March 2020 , Volume 7 Issue 2*

Disaster Response *By Peter Aggus*



The world is reeling from what disaster planners feared: a viral pandemic. So, how are those "best laid plans" faring? Is everything working like clockwork, as it was planned to? Are we learning from the challenges we face? Disasters do not wait for a more convenient time. Are we ready for a second disaster that could strike while we are still trying to deal with the first? They said "smile—things could be worse. " So I smiled … and things got worse.

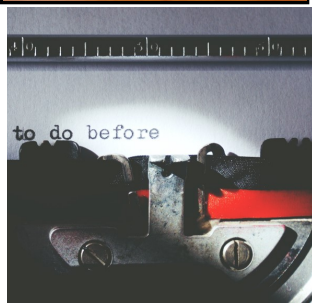
The 4th Industrial Revolution *By Ellen Koskinen-Dodgson*

Covid-19 has shaken up everyone's lives and forced us to go more deeply online. One of the interesting consequences will be the speeding up of our move to the 4th Industrial Revolution. According to the Encyclopaedia Britannica, "By affecting the incentives, rules, and norms of economic life, it transforms how we communicate, learn, entertain ourselves, and relate to one another and how we understand ourselves as human beings."

Pro-Bono Offer for School Districts

TMC has decided to donate our expert advice to school districts in need. We would like to assist you as you make the transition from classroom learning to online education, and help you with any problems you may experience along the way. TMC consultants include instructors who use online learning platforms and engineers with considerable knowledge of collaborative learning environments. If this might be of interest to you, feel free to contact Ellen at ellen@tmcconsulting.ca.

Your Disaster Plan is Incomplete *By Guy Robertson*



No disaster plan is perfect. All plans contain weaknesses and gaps, some of which could accommodate unexpected perils. For example, numerous plans in California have prepared organizations for earthquakes, power outages, and wildfires but not for the novel coronavirus pandemic of 2020. In New York City and London, corporate plans have justifiably concentrated on terrorist attacks and severe weather, but often include no mention of pandemics.

Evolving Cloud Threats *By Elleni Koskinen*

Last year Symantec published the Cloud Security Threat report to assist companies in identifying cloud based security threats. They found that many of these threats existed as a result of the company's own misuse and misunderstanding of cloud based work. With over half of the average organization's workload now occurring in the cloud, it's time to get serious (and get educated) about cloud security.

 ISSN 2369-663X

Disaster Response *By Peter Aggus*

The world is reeling from what disaster planners feared: a viral pandemic. So, how are those "best laid plans" faring? Is everything working like clockwork, as it was planned to? Are we learning from the challenges we face? Disasters do not wait for a more convenient time. Are we ready for a second disaster that could strike while we are still trying to deal with the first? They said "smile—things could be worse. So I smiled ... and things got worse."

COVID-19

The doomsayers (i.e. those of us in disaster planning) said we could get a pandemic viral outbreak—and so we have. However, this is not the time to be smug and say "told you," but rather it is the time to say "look, the plans we made work" ... but do they?

Disaster plans need to be flexible. We may know the basics of how disasters start, but we can rarely control how or when they will end.

Teleworking

Are you one of the many companies whose disaster plan called for teleworking? If so, you are in good company. However, if the plan was not fully tested in advance, you may be in for some surprises.

Here are some of the issues faced:

Insufficient VPN ports

Most IT departments set up inbound VPN servers to cope with approximately 10% of key workers connecting from off-site. What happens when management says 100% need to?

Too little datacentre bandwidth

Many organisations run cloud or virtualised applications where the data traffic between client and network can

be quite high. If you only tested VPN access using local applications you may be in for a shock with bandwidth demands. A VPN connecting offsite is not the same as a 1Gbps local connection.

Too few remote licenses

Do your application licenses cover enough off-premises users? All too often the answer is no.

Laptops not up to the job

We saw several companies who use laptops for portability with desktop docking stations or port extenders in the office. The employee can take the processor home and VPN back to the office for access to application and data—but what about screens? That port extender often has two 27" screens attached that are normally used for all the windows needed at work. The laptop alone may be fine for email and word processing but not the whole job. And without admin rights, the employee can't install the drivers for their own port extender.

Domestic internet service has too little bandwidth

Home users' network speeds may work well for personal email, but are often overburdened by corporate needs.

Nested Disasters

Have you considered that we could have another disaster before COVID-19 ends? Earthquakes strike with no warning. Does your disaster plan cope with the fact that you might already be in "disaster mode"? Staff may be working remotely, so will they be able to respond as the plan expects?

Ongoing Adaptation

As the crisis develops, you need to monitor how well your disaster plans are working and adapt as needed.

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

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

The 4th Industrial Revolution *By Ellen Koskinen-Dodgson*

Covid-19 has shaken up everyone's lives and forced us to go more deeply online. One of the interesting consequences will be the speeding up of our move to the 4th Industrial Revolution. According to the Encyclopaedia Britannica, "By affecting the incentives, rules, and norms of economic life, it transforms how we communicate, learn, entertain ourselves, and relate to one another and how we understand ourselves as human beings."

Building On...

The first industrial revolution was steam and water driven machines. The second was electricity and mass production, and the third was IT systems and automation. Each of these revolutions caused massive economic and cultural disruption, both positive and negative; nations became wealthier while some subgroups suffered greatly. Time will prove if this will also be true for the fourth industrial revolution.

Is it 4 or 3+?

The fourth differentiates itself from the third in a number of ways. First, the evolution of technology is increasingly accelerating in speed from the third, or digital, revolution from which we are transitioning. Second, these evolving and new technologies are merging with our physical lives with examples such as smart-watches and autonomous cars. Other differentiators include required government changes – for example, how do we regulate and tax technology when it may be dispersed around the globe?

What Does it Include?

Many technologies bleed between third and forth like simple Internet of

Things, facial recognition and early AI. Transitioning into fourth sees solutions that combine various new technologies and human interaction interfaces indistinguishable from interactions with a person. Technologies can include impressive AI, properly autonomous vehicles, blockchain technology for money and other types of transactions, voice activated assistants, drones, genome editing, robotics, augmented reality and more.

COVID-19 Impact

Efforts to manage the spread of Covid -19 have led to governments around the world asking most people to stay home for an unspecified period, working from home if they can and finding at-home ways to amuse themselves if they can't. School boards and students are being asked to find ways to complete their curriculum for the year on-line. All of this will lead to an increased acceptance of online work, education, socializing, and entertainment. It will also be fertile ground for clever people with too much time on their hands.

Looking Forward

People, companies and governments will all need to change their behaviours, often in major ways, just like in previous industrial revolutions. There will, as before, be winners and losers, and most predictions of the future will be wrong as major disruptors are rarely predicted.

I recommend that you include time spent in forward-looking speculation and investigation as part of your annual strategic planning exercises, as those that do this will greatly increase their chances of succeeding in the fourth industrial revolution.

This article is reproduced from the March 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.

Your Disaster Plan is Incomplete *By Guy Robertson*

No disaster plan is perfect. All plans contain weaknesses and gaps, some of which could accommodate unexpected perils. For example, numerous plans in California have prepared organizations for earthquakes, power outages, and wildfires but not for the novel coronavirus pandemic of 2020. In New York City and London, corporate plans have justifiably concentrated on terrorist attacks and severe weather, but often include no mention of pandemics.

Your Toolbox is Empty

Even after the outbreaks of SARS and H1N1 influenza, planners frequently ignored widespread outbreaks of disease when they revised their plans. Emergency telephone directories were updated, along with equipment inventories and IT security protocols, but when the morbidity of COVID-19 increased worldwide, managers in countless organizations discovered that they were not prepared. When they opened their disaster (or business resumption, or continuity) plans they discovered that, while they were prepared for high winds and hostile intruders, they had little protection against the most dangerous intruder ever to threaten many of them. Invisible and unpredictable, the novel coronavirus might not be as lethal as the Black Death or other outbreaks of plague, but it has caused tens of thousands of deaths, enormous social anxiety, and serious problems for the global economy.

Panic is Spreading

Frightened people have hoarded staples and cashed in their investments against the advice of government authorities and financial advisors. All over the world people

wonder what course the coronavirus pandemic will take. When will it end? How many people will fall ill? Nothing seems certain. But good advice is available in the form of directives from health care authorities. They urge people to protect themselves through measures including:

- Frequent handwashing
- Social distancing
- Working from home

Encouraging your employees to prioritize their health and safety may help to lessen feelings of anxiety, and avoid mass panic. After all, in times of trouble panic is often more dangerous than the original cause.

Who's Next?

A standard part of pandemic management is succession planning. Many organizations have plans in place should the CEO or other senior managers become unexpectedly unavailable. But key employees such as IT systems experts, laboratory managers, and accountants often have nobody to replace them should they become unable to work. Without them and other key employees, organizations could shut down for indefinite periods. The temporary unavailability of one key employee could result in reduced market share, loss of customer confidence, and cash flow problems. Hence succession planning has become a key piece of pandemic management planning.

Be Ready for Next Time

Now we must deal with COVID-19, but experts predict another pandemic in the not-too-distant future. Are you and your employees prepared? Will you be ready when your office is shut down (again)? It's time to fill that gap in your disaster plan.

This article is reproduced from the March 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.

Evolving Cloud Threats *By Elleni Koskinen*

Last year Symantec published the Cloud Security Threat report to assist companies in identifying cloud based security threats. They found that many of these threats existed as a result of the company's own misuse and misunderstanding of cloud based work. With over half of the average organization's workload now occurring in the cloud, it's time to get serious (and get educated) about cloud security.

Perception vs. Reality

The vast majority of organizations currently using the cloud have trouble keeping track of their workload. In fact, most employers drastically underestimate the real number of cloud-based apps that their company and their employees are using (on average the number of apps is four times higher than what they expected). With no tangible understanding of what work is happening or how it gets done, it's no wonder that so many businesses experience cloud security threats.

Are We Trained for This?

With businesses becoming more cloud based every day, it only seems logical that employees would be getting more cloud savvy as well. However that's not the case. 93% of employees that were surveyed said that they lacked the necessary security skills, and the majority of participants believe that inadequate cloud security practices are the cause of cloud security incidents. And if you're wondering how prevalent cloud incidents are, they made up almost 2/3 of all security incidents in 2018.

Risky Business

Over 1/4 of employees engage in "risky business." That is to say that they misuse cloud applications in a way that puts their organization's sensitive data at high-risk. However, what is perhaps more alarming is that almost all users are putting corporate data at risk by inadvertently oversharing. Insider threats, whether purposeful or accidental, are occurring with increasing intensity. The worrying result is that 68% of survey participants have seen direct or likely evidence that their data has been made available for sale on the dark web.

Cloud Apps

Symantec internal data reports that of the ~33,000 apps that the Business Readiness Rating has reviewed, a mere 1% have the required built-in security for regular business use, and 39% of them are not suitable for business use at all. Being more selective (and more knowledgeable) of which applications have access to your networks and your data will go a long way in protecting your business.

Next Steps

Education is the best weapon against security threats, and with 85% of users not using the Center for Internet Security's best practices, we could all use it. Here are Symantec's top 4 suggestions for improving security:

1. Develop a strategy supported by a Cloud Center of Excellence (i.e. a team of people responsible for managing the cloud).
2. Embrace a zero-trust model.
3. Promote shared responsibility.
4. Use automation and AI wherever possible.

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

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