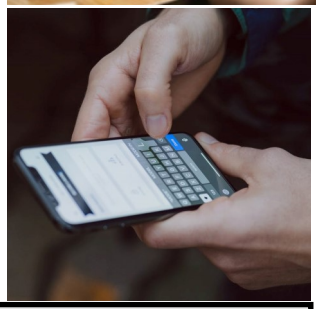
TMC's ADVISOR

Covering IT and Telecom from a Canadian Viewpoint — *Sept 2019 , Volume 6 Issue 2*

Security Scare Tactics Don't Work *By Ellen Koskinen-Dodgson*

If your executive team doesn't support your cyber-security program, the likelihood of disaster increases. For everyone's sake, you need to convince them to take your recommendations very seriously. Unfortunately, they don't speak tech, and they can't be scared into understanding. So how do you convince your executive to see cyber-security for what it is?

Ten Trends You Need to Know *By Lee-Ann Dittrich*



Gartner has identified ten trends with the most potential to transform industries in the next 5 years. The trends will be introduced here, but must be examined more thoroughly through a business lens in the coming months. The top trends fall into three categories. Gartner calls them "Intelligent," "Digital," and "Mesh." They mean evolving tech intelligence, cool technology advances, and game-changing ideas. Are you ready? The future is already here.

Disaster Recovery Checklist

If you answer NO to any of these questions, you need to revisit your business continuity plan:

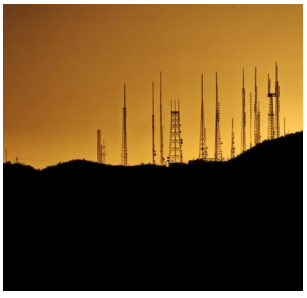
- Does your plan address succession planning for key staff?
- Does your plan include flags for when it needs to be updated?
- Does your plan include emergency communications with key clients?

For a more comprehensive list, request our checklist by contacting Ellen at ellen@tmcconsulting.ca.

Afraid of the Dark Web? *By Elleni Koskinen*

Hackers are an ever-evolving breed, becoming stealthier and more resourceful with each passing year. The Symantec Internet Security report takes a look at the past year to identify trends, threats, points of entry, and practices that may put your business at risk. Whether you're online to reorder office supplies, emailing with a colleague, backing up into the cloud, or just conducting business as usual, you may not be as safe as you think you are.

5G Rollout *By Peter Aggus*



In the last issue, Tony looked at "The 5G Conundrum" and explained some of the technology issues faced by 5G deployment as well as some of the claimed benefits that we look to enjoy. So is 5G here yet? Or is it forever on the horizon? We take a look at progress and expectations as well as whether the hype is really justified—or even necessary. To some, 5G is still "a solution looking for a problem."

 ISSN 2369-663X

Security Scare Tactics Don't Work *By Ellen Koskinen-Dodgson*

If your executive team doesn't support your cyber-security program, the likelihood of disaster increases. For everyone's sake, you need to convince them to take your recommendations very seriously. Unfortunately, they don't speak tech, and they can't be scared into understanding. So how do you convince your executive to see cyber-security for what it is?

Avoid IT-Speak

Don't speak of botnets, brandjacking, catfishing, darknets, DDOS attacks, pharming, (spear) phishing, ransomware, whaling and all of the other cool words that you know. If they ask about one of these words, be prepared to define it, but otherwise stick to business language.

Use Their Language

The C-suite and board members are business people who think in business terms like "value" and "ROI." Value can include compliance, data confidentiality, protection of intellectual property and systems availability.

While the ROI of security is difficult to quantify, it's the same with insurance costs, and senior management understand the value of insurance even if it's also hard to put into ROI terms. They know that "perfectly secure" isn't doable in the real-world and that chasing that goal can be cripplingly expensive. They understand that they will need to balance risk vs. cost. Help them do that.

Help Them Decide

Help them understand enough to assess the risk:

- Explain your recommended program and the trade-offs between cost and improved security.
- What is the organization's most sensitive data? How will it be treated differently than the rest of the data?
- What is the cost of system or data loss?
- Explain that monitoring is in place to detect and stop emerging risks and how effective that monitoring will be.

After a Breach

Security breaches will happen, so have the presentation mapped out in advance. In fact, it should be included in the business continuity/disaster recovery reporting process. If it's not already part of your plan, now is the time. After all, when you're dealing with a breach, you'll have no inclination to start writing then.

BCP/DR Advice

That said, when is the last time you updated or tested your business continuity/disaster recovery plans? You should consider BCP/DR to be a program (rather than a plan) that can be written, then ignored. When you need it, it must work and can't be out of date. Put testing and updating on your calendar at least once per year.

We encourage our clients to test and review segments of their BCP/DR plans on a quarterly basis. This keeps the topic a little closer to front of mind without quadrupling the work.

This article is reproduced from the September 2019 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.

Ten Trends You Need to Know *By Lee-Ann Dittrich*

Gartner has identified ten trends with the most potential to transform industries in the next 5 years. The trends will be introduced here, but must be examined more thoroughly through a business lens in the coming months. The top trends fall into three categories. Gartner calls them "Intelligent," "Digital," and "Mesh." They mean evolving tech intelligence, cool technology advances, and game-changing ideas. Are you ready? The future is already here.

Intelligent

1. Autonomous things can interact with their environment more naturally than ever to ease the burden of tedious, specific tasks. Coming soon to your company car or office coffee machine.

2. Augmented analytics means that businesses can spare the hefty price tag of expert data scientists and still generate the key insights into their products and customers.

3. AI-driven development allows developers to generate applications (even if they have no coding knowledge) by using premade AI tools. Gartner estimates that 40% of new application development projects will have AI co-developers by 2022.

Digital

4. Bringing power to the edge: empowered edge technology will allow connection and processing to occur closer to endpoint devices. This will reduce traffic and latency by reducing the need for IoT devices to connect to a centralized cloud.

5. Immersive technologies will allow the user to be connected to the

digital world by devices all around them. From cars, to watches, to sensors, the days of connecting to the computer are gone, as very soon we will be living within it.

6. Quantum computing, although still in the emerging state, will have the capacity to solve problems that are too complex for traditional systems to deal with. Now is the time to learn about it.

Mesh

7. Blockchain is an online public record with a variety of applications. Everything is transparent and traceable, and it makes tasks like accounting, which are culpable to human error or fraud, all but foolproof. Australia has committed to using Blockchain operations for their stock exchange, and Moscow is adopting the technology for municipal elections.

8. Smart spaces are environments in which people and technology interact to create a harmonious experience for the user. Smart homes and digital workplaces will continue to multiply in the next 5 years.

9. Digital ethics and privacy have become focal points for users. Customers are more knowledgeable about their privacy rights, and are demanding that every interaction be grounded in ethical digital practices.

10. Digital twins are complicated virtual models of real life physical things, such as cars or power plants. They use IoT sensors in real-time to feed back into the model. Digital twins for organizations (DTO's) will digitize the company's business model and practices, and DTO's will be able to respond to problems automatically.

Lee-Ann is a researcher and business analyst.

This article is reproduced from the September 2019 edition of ***TMC's Advisor***

Afraid of the Dark Web? By Elleni Koskinen

Hackers are an ever-evolving breed, becoming stealthier and more resourceful with each passing year. The Symantec Internet Security report takes a look at the past year to identify trends, threats, points of entry, and practices that may put your business at risk. Whether you're online to reorder office supplies, emailing with a colleague, backing up into the cloud, or just conducting business as usual, you may not be as safe as you think you are.

The Shopping

The use of malicious JavaScript to collect credit and debit card information, known as formjacking, rose in 2018, and it's easy to see why. E-commerce sites are lucrative targets for hackers. Payment card information can sell for up to $45 per card, and with almost 5000 unique websites compromised each month in 2018, that can easily equate to millions in ill-gotten gains. Formjacking attacks generally targeted third party services, which are often weak points for even the most well protected websites. Chatbots and "leave a review" widgets, which are especially common on e-commerce sites, were the most frequently attacked. The hackers would often exploit routine software updates by injecting malicious code into the legitimate programming, leaving the developer and the user unaware of the threat. Formjacking attacks can affect any business that accepts payment online, and no size of business is exempt from the risk.

The Mail

In Canada last year, Microsoft Office files accounted for almost half of all malicious email attachments,

showcasing a worrying trend of hackers solely using software that is generally found on most computers. "Living off the land," as it's called, doesn't require additional code or software, but uses Office files laced with malicious script as a gateway to gain access, then downloads malware once the attachment has been opened. This tactic puts even the most security conscious users at risk, as the emails are often disguised as receipts, or even legitimate work communication with correspondingly appropriate file types.

The Cloud

Cloud databases were also found to be weak points, although hackers shouldn't take as much credit for that, as much of the security risk was due to user error. Poor cloud configuration led to over 70 million records being compromised in 2018.

The Things

Another risk area was established with the rise of the Internet of Things. Physical devices with less stringent security and the ability to connect to networks allow hackers an ideal point of attack. Routers, cameras, printers, and even alarm systems were common targets in 2018, opening the door for hackers to compromise operation computers, and possibly mount disruptive operations.

The Counter-Strike

Education is the best weapon against these cyber-attacks. Having an understanding of how hackers can gain access to confidential information allows us to take the appropriate steps to prevent it. Hackers may be an ever-evolving breed, but we can be too.

This article is reproduced from the September 2019 edition of *TMC's Advisor*

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

5G Rollout By Peter Aggus

In the last issue, Tony looked at "The 5G Conundrum" and explained some of the technology issues faced by 5G deployment as well as some of the claimed benefits that we look to enjoy. So is 5G here yet? Or is it forever on the horizon? We take a look at progress and expectations as well as whether the hype is really justified—or even necessary. To some, 5G is still "a solution looking for a problem."

5G Simplified

5G is actually two separate things. Firstly it is a signalling protocol standard that is an evolution of what is used in 4G networks. Secondly it is a new set of radio frequencies providing more bandwidth, most of which are at much higher frequencies.

It's the new frequencies that are proving to be quite controversial.

New Territory

Frequencies above 30 GHz have never been used for wide area communications. 5G objectors point out that the 5G millimeter waves are very close to those used by the US Army in their crowd dispersal guns which generate an intolerable heating sensation until a person moves out of the beam. Some suggest that our current radio frequency safety standards will need to be revisited.

The Real World

Practical experience in trials is not matching theory nor is it as good as the demo installations that heralded a great new era. Clearly there are real world issues that need to be better understood before we are ready for major rollout.

There are also an increasing number of jurisdictions that are refusing

permission to widely deploy millimetre wave cell sites. Perhaps coincidentally, many of these jurisdictions have deployed wide area WiFi with a business model that will be impacted if 5G cellular were allowed to compete.

Several court cases are underway—all of which focus on alleged safety issues of millimetre wave radio frequencies.

Another Approach

It turns out that 5G protocols can be used with some existing 4G frequencies and networks without tackling the technology and range issues of Hi-Band "millimetre waves."

Low- and Mid-Band frequencies are better understood. The former serve our current 4G LTE networks and the latter are used for WiFi.

Once the technology is shaken down, it is likely that we will get better performance from 5G using the old 4G infrastructure (cell towers and backhaul network) to support rapid rollout is engineered.

The downside is that lower frequencies do not easily lend themselves to the "blistering network speeds" users are expecting from 5G.

The Future

Clearly the industry sees a need for 5G as users data usage continues to escalate. In the near-term, most demands can be met by evolving proven 4G technology and extending it into "Wi-Fi like" mid-band frequencies around 6GHz.

The new >30 GHz frequencies can deliver focussed applications to moving vehicles in limited areas but the case for the much hyped 5G urban 100m cell site grid could prove stillborn.

This article is reproduced from the September 2019 edition of ***TMC's Advisor***

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