Mark W. Baker, MA, FCIP, CIP, CRM, CBCP, MBCI
Risk and Insurance Management
Business Continuity Consultant
Phone: (416) 261 4963
Fax: (416) 261 7685
Email: BCPRiskManagement@bell.net
Web: www.BCPRiskmanagement.ca

CYBER RESILIENCE - **IT'S NOT JUST** THE COMPUTERS

WHAT I AM GOING TO TALK ABOUT

- Introduction
- Look at *some* of non cyber threats/risks to your IT operation
- How to classify these threats/risks
- Ways to acquire data to assess these risks
- How to use it to assess risk

INTRODUCTION

Who am I

- Mark has over twenty years' experience in Business Continuity Planning, IT Disaster Management, Risk Assessment, Enterprise Risk Management as well as Disaster and Emergency Management for organizations ranging from large corporations to small businesses. He has developed and tested many business continuity and IT disaster recovery plans as well as creating and administering exercises varying from table top to full scale exercises.

  Mark has been involved in the response and mitigation of many disasters working on over twenty events including the Quebec/Ontario ice storm and the Peterborough flood. Recently, he has served as Co-chair of the Private Sector Working Group and member of the advisory board for Canada's Platform for Disaster Risk Reduction. He has published several papers on subjects ranging from the effects of climate change on insurance to risk management and biotechnology.

  He is a graduate of Royal Roads University with an MA in Disaster and Emergency Management and the University of Toronto with a BSc in Physical Geography. Mark is a Fellow Chartered Insurance Professional (FCIP), holds a Certificate of Risk Management (CRM), a Certified Business Continuity Professional CBCP and is a Member of the Business Continuity Institute (MBCI) as well as a former officer in the Canadian Navy…*fancy way of saying*

- I have done a lot of risk assessments

INTRODUCTION

- Cyber threats – Major problem today
  - Very recently – WannaCry Ransomware
- Not just the super hacker from Russia (North Korea)
- Non Cyber Threats to your IT Facility and operation
  - May be as important as cyber threats themselves
  - May exacerbate the cyber threats
- What is a risk, what is a threat, we will not get into this today

INTRODUCTION

- This is not an exhaustive list
  - Have to keep updating your risks, hazards and responses
    - Always keep learning always stay up to date
- A methodology to be applied
  - Have to keep updating your methodology or methodologies
- Not the only way to do this, there are other methodologies
- Only an introduction with some examples

CLASSIFICATION

- Different ways of looking at the problem – types of risk
- Where are your risks?
  - Locational risks – related to where your IT centre is
    - Site of location (issues either at the location or very close)
    - Situation of the location (General Geographic areas)
  - Non locational risks - Business/psychological
- What creates your risks?
  - Natural (created by the natural environment mostly)
  - Human (created by us…mostly)
- The above all interrelate

CLASSIFICATION

- Yes, it all interrelated… so you can have
  - Natural Locational Risks, Human non-locational risks, Human locational risks etc.
- Yes, there is overlap. Are risks that arise from anthropogenic (human based) climate change human or natural. Well in some ways both.
  - Don't get too hung up on which bucket something is in. Just make sure it is understood and assessed.
    - By the best person in the organization
      - It may not be you (May be the Enterprise Risk Manager or the Security Supervisor)

CLASSIFICATION

- Locational Risks

We can also talk about the site and situation of an IT centre/location (adaption of geographic terms, not exactly the same)

- Site is the actual location of an IT Centre/Location and its physical characteristics and what is close to it
  - Close to the ocean, a river or a G20 event
- Situation are characteristics of the general area
  - Ontario snow characteristics

CLASSIFICATION – A FEW DETAILS

- Natural
  - Usually Locational in nature – therefore Geographic
    - Hydro-climatic - Has to do with the climate and its results
      - Hurricanes, Tornadoes, Mid-latitude storms, floods,
    - Geological – Has to do with the earth
      - Earthquakes, Tsunamis
    - Ecological – Has to do with the ecosystem
      - Forest Fires
    - Space Weather (may not be locational sort of)
- Human
  - Sometimes locational in Nature
    - Issues around your IT centre
      - Your neighbours (embassies)
      - Human activities (G 20 conference, fun runs, parades, protests)

CLASSIFICATION – A FEW DETAILS

- Human – sometimes NOT locational (at least not completely)
  - Standards you use (May not be your choice)
  - Regulatory/Legal/Jurisdictional issues (quasi-geographic)
  - Human resources policies

HOW TO ASSESS – SOME EXAMPLES

- Locational Site Based Risks
  - Human
    - Building itself – Just some examples, things to look for
      - Physical Characteristics and Security
        - Locks (1 million dollars of Cyber Security protected by a $5 dollar lock)
        - Security Guards (Are they there, are they needed, what do they do, training?)
        - Alarms
        - Access Control to your spaces

HOW TO ASSESS – SOME EXAMPLES

- Locational Site Based Risks
  - Human
    - Building itself – continued
      - Sprinkler systems/Fire Suppression
        - Could damage servers?
      - Back up power
        - Diesel or Gas Generators (Condition of these spaces)

HOW TO ASSESS – SOME EXAMPLES

- Locational Site Based Risks
  - Human
    - Building itself – A few more (many of you probably know some of this)
      - Physical Security/Characteristics cont.
        - Backup communications (more than one set of phonelines coming in)
          - Cell phones…do you have enough cell coverage
          - Satellite phones…do you have line of sight
        - IT spaces are in the…
          - Basement (below a sewer line), Top Floor (Snow Load)

HOW TO ASSESS – GETTING INFORMATION

- Locational Site Based Risks – How to assess
  - Human- Building Itself
    - Simply look around, get out from behind your desk (or out of the data centre)
      - Not just in the building, walk around outside…it's a best practice
    - Many text books on all previous (LAST Resort far better to do the next set)
      - Don't do this all yourself, there are experts out there in YOUR organization
    - Other departments at your organization
      - Talk to other departments in your company, again get our of your office
        - ERM, Risk and Insurance Management, Security, Compliance…employees!!!
      - Create organization wide risk committees, interdepartmental risk registers, ERM (Enterprise Risk Management)…dovetail into all of this.

HOW TO ASSESS – GETTING INFORMATION

- Locational Site Based Risks – How to assess
  - Human Building Itself (cont.)
    - Your insurance company (Work with your Risk and Insurance Management Dept.)
      - Field underwriter at insurance company may already have done this and may have good suggestions (often are engineers)
    - Talk to your Landlord, Police, Fire Department, Municipal Emergency Management Department

HOW TO ASSESS – SOME EXAMPLES

- Locational Site Based Risks
- Things to look for
  - Human - Just Outside the Building
    - Who are your neighbours
      - Embassies, Consulates and Universities
        - Protests, possibly terrorism
      - Sports Stadiums
        - We Won!!! Or Lost (think sports riot in Vancouver)
      - All of the above could damage your data centre (or just prevent people getting there

HOW TO ASSESS – SOME EXAMPLES

- Locational Site Based Risks
  - Human- Just Outside the Building (cont….what else is close)
    - Generally being at the Centre of it all
      - Santa Claus Parade
      - G20
      - Marathon fund raising
    - All of the above may prevent people and material getting to your data centre
      - Perhaps should not be at the centre of it all
    - Infrastructure such as Highways, Airports and Railways
      - Dangerous cargos…potential damage in injury
    - Plain old crime

HOW TO ASSESS – SOME EXAMPLES

- Locational Site Based Risks
  - Natural - Just Outside the Building – Look for
    - Streams, Flood Plans, Oceans, Forests
    - Potential Landslides
    - Yes I have seen all of these

HOW TO ASSESS – SOME EXAMPLES

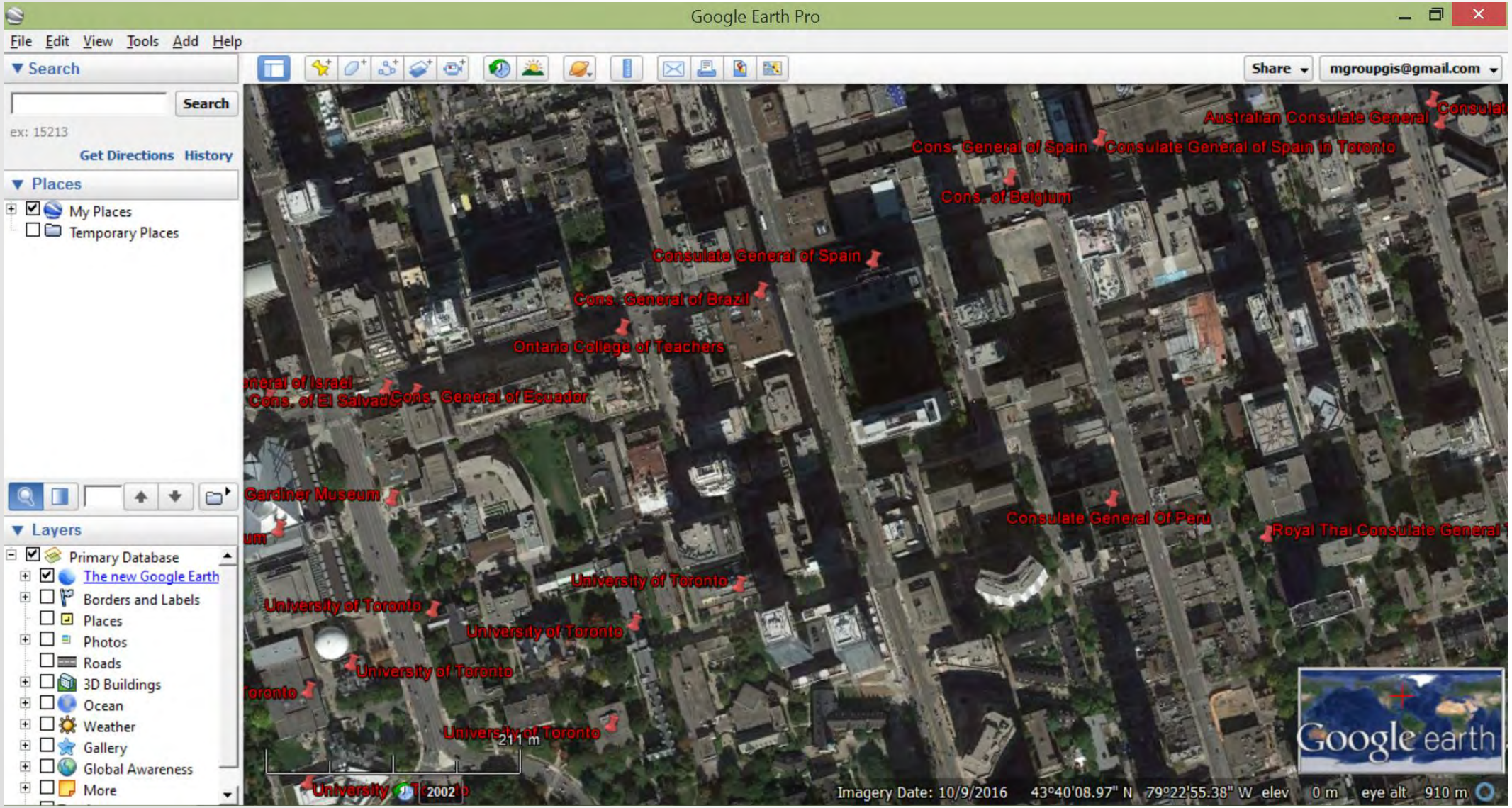
- Locational Site Based Risks – How to assess
  - Natural AND Human
    - Simply look around, get out from behind your desk/data centre
      - Walk Around Outside…again (In geography it is called ground truthing)
    - Talk to the same people as in previous slides
      - Fire
      - Police
      - EMS

HOW TO ASSESS – SOME EXAMPLES

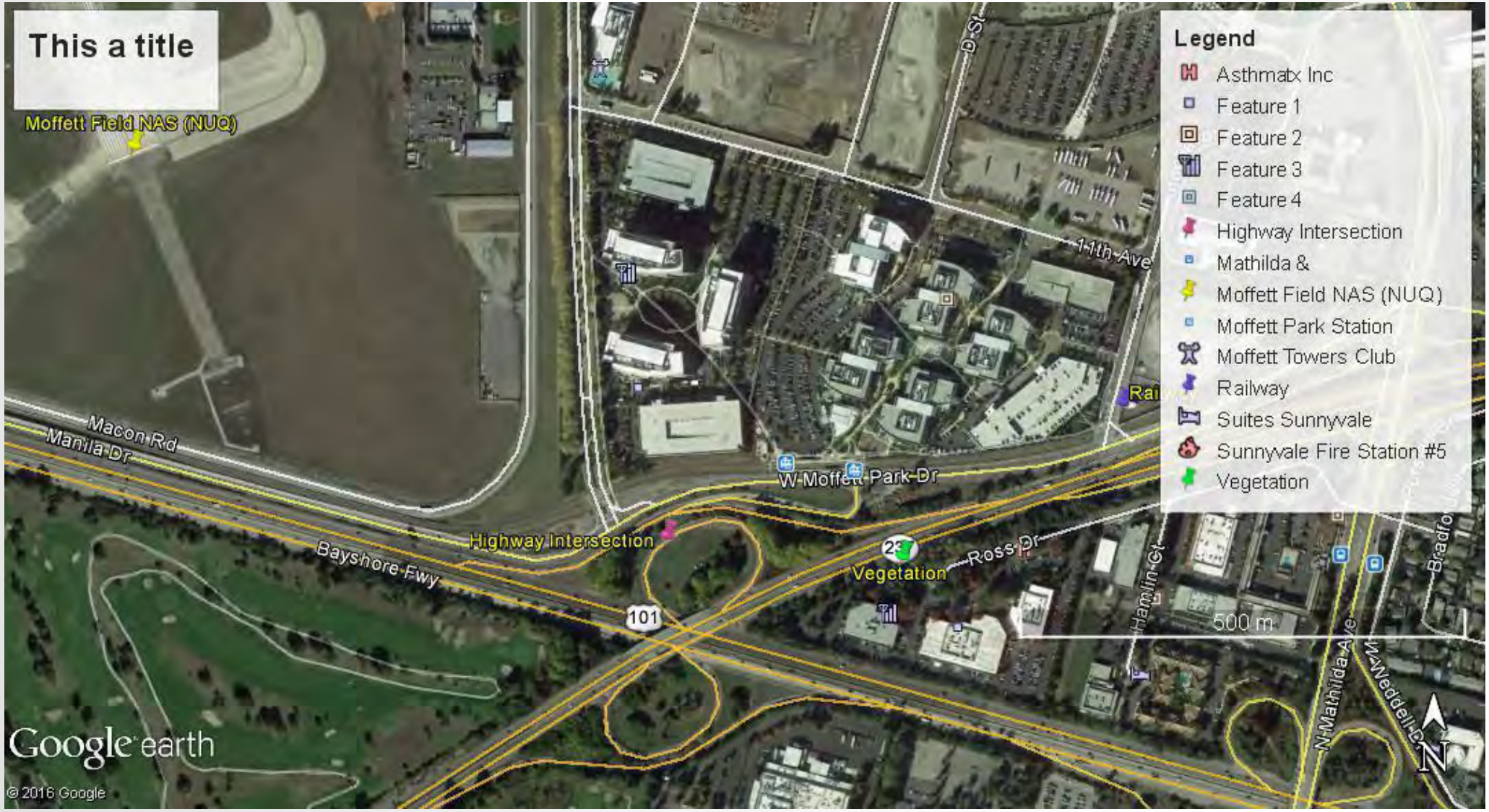
- Locational Site Based Risks – How to assess
  - Your new best friend – Google Earth Pro – Its FREE!!
    - And, within limits Wikipedia
    - Good (though limited GIS, Geographic Info system)
    - https://www.google.ca/earth/download/gep/agree.html
    - Tough to screw up
      - BUT untrained users can make mistakes in scale, projection with GIS
        - If you are not trained, stick with their data
        - Not perfect, not everything is found, be sceptical

HOW TO ASSESS – SOME EXAMPLES

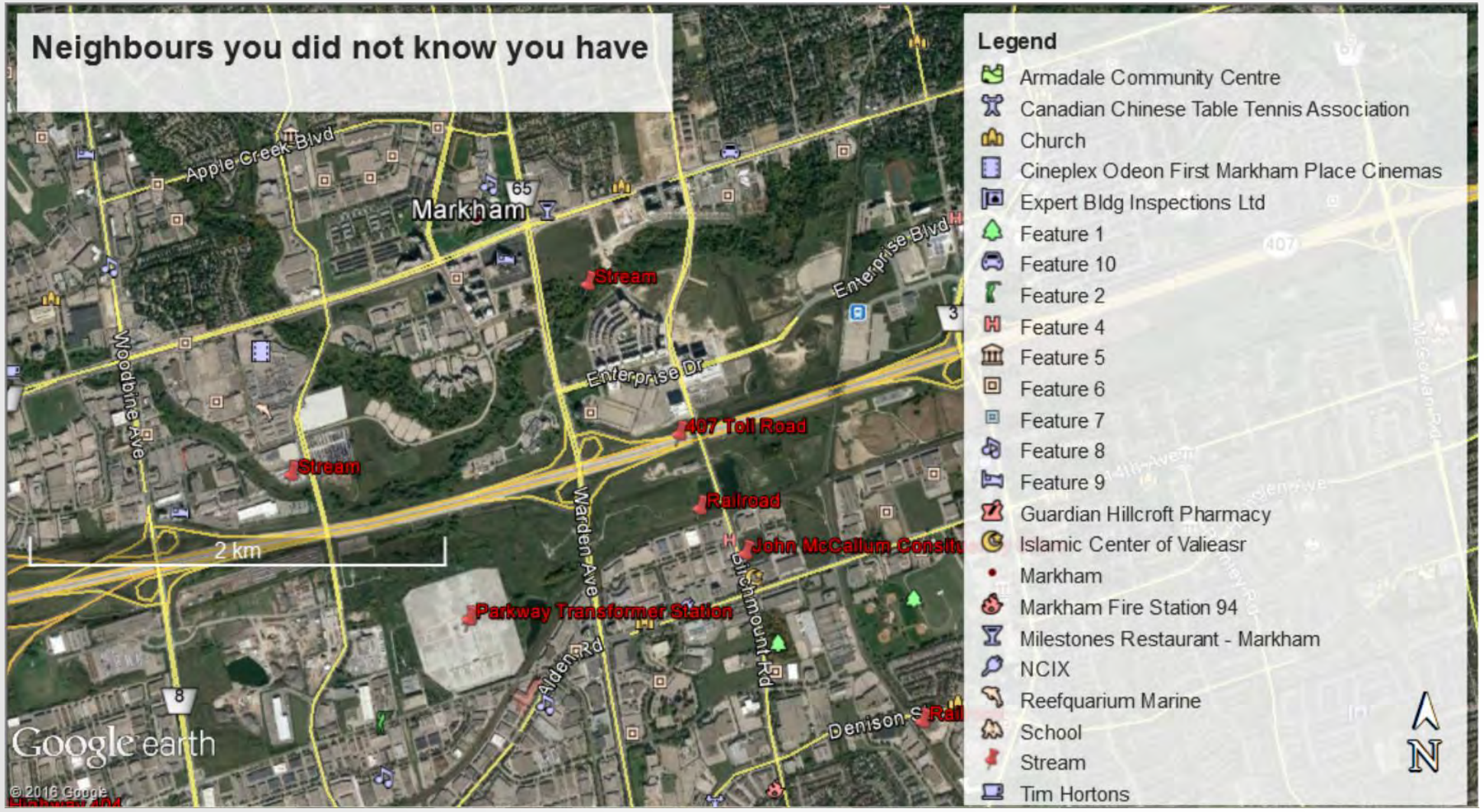
- Google Earth slide



HOW TO ASSESS – ANOTHER EXAMPLE



HOW TO ASSESS – YET ANOTHER EXAMPLE



HOW TO ASSESS – SOME EXAMPLES

- Locational Situational Based Risks –
  - Risks in General Area
  - Natural
    - Hydro-climatic - Has to do with the climate
      - Hurricanes, Tornadoes, Mid-latitude storms, floods,
    - Geological – Has to do with the earth
      - Earthquakes,
      - Tsunamis
    - Ecological – Has to do with the ecosystem
      - Forest Fires
  - Man Made Geopolitical Risks
    - Issues Around the World that come back here (Situation affecting Site)

HOW TO ASSESS – SOME EXAMPLES

- Information Sources – Natural
  - Natural Resources Canada - https://www.nrcan.gc.ca/home
    - Join Hazus Canada www.hazuscanada.ca
      - Malaika Ulmi malaika.ulmi@canada.ca
  - CRHNet (Canadian Risk and Hazards Network)
    - http://www.crhnet.ca/
  - Conservation Ontario
    - http://conservationontario.ca/
  - Institute for Catastrophic Loss Reduction (Insurance Industry)
    - https://www.iclr.org/

  - Your Local Municipality
    - Same people as before

HOW TO ASSESS – SOME EXAMPLES

- Information Sources – Human
  - The News, not great but at least you will eventually know what is going on
  - Open sources Intelligence sites – What event will cause the next protest in your area
    - Geopolitical Futures - https://geopoliticalfutures.com/
    - Stratfor - https://www.stratfor.com/
    - The Strategy Page (very military) - https://www.strategypage.com/

HOW TO ASSESS – SOME EXAMPLES

- Information Sources – Human (cont.)
  - Pandemic Sites (your people are your greatest asset, sick coders can't code)
    - Public Health Agency of Canada
      - http://www.phac-aspc.gc.ca/index-eng.php
      - World Health Agency
      - http://www.who.int/en/
  - Your Local Municipality
    - Same people as before

HOW TO ASSESS – SOME EXAMPLES

- Again you can map this info
  - Use care in using a Geographic Information System (GIS). Too little time to detail problems(use a professional?)
- Manifold…a good cheap GIS
  - Not perfect, need GIS skill set

    http://www.manifold.net/
- Can also pull data from Google Earth and drop it in
- Snow Storm Issues for all locations

HOW TO ASSESS – NON LOCATIONAL

- Usually Human –NOT locational (or mostly Not-locational)
  - Standards you use (May not be your choice)
    - Compliance or Non Compliance with a standard may cause you problems
    - Creates legal issues that affect your configurations, your data storage and your applications
  - Regulatory/Legal/Jurisdictional issues (quasi-geographic)
    - Same and relates to the above as above but can be more severe
      - Records Storage ruling can affect how long and how you will destroy your data
    - Multiple Jurisdictions may mean overlapping effects

HOW TO ASSESS – NON LOCATIONAL

- Human resources issues
  - Your Employees,
  - Who do you hire, how much do you pay them?
    - You may be "giving them the keys to the kingdom"
    - If someone talented is working for minimum wage, why are they doing that?
    - Are you creating issues? Do due diligence
  - Pay your employees what they are worth

HOW TO ASSESS – NON LOCATIONAL

- Human resources issues
  - Your Employees
  - New Hires
    - If someone is doing patches and upgrades, should not give full access to all systems and data bases
    - New Hires should be on Probation until they prove themselves.
  - Cross training is GREAT, especially in times of disaster
    - However tailor so that it can be activated only at the time of a disaster

HOW TO ASSESS – NON LOCATIONAL

- Human resources issues
  - The Organizations employees as a whole e.g..
    - Salespeople
    - Data Entry
  - Don't let security overwhelm them
    - The password &8872$*$ksdj3 changed every week is not an option
    - Educate all employees on the basics of cyber security and make them part of the solution

HOW TO ASSESS – NON LOCATIONAL

- Human resources issues
  - The Organizations employees as a whole cont.

    - Account for the phycology of your employees
      - Cognitive load
      - Realistic expectations

HOW TO ASSESS – NON LOCATIONAL

- Human resources issues
- On these issues I recommend anything by Shari Lawrence Pfleeger

- Shari Lawrence Pfleeger, M. Angela Sasse and Adrian Furnham, "From Weakest Link to Security Hero: Transforming Security Staff Behavior," Journal of Homeland Security and Emergency Management , 11(4), October 2014,pp. 489-510.
- Shari Lawrence Pfleeger and Deanna Caputo, "Leveraging Behavioral Science to Mitigate Cyber Security Risk," Computers and Security , 31(4), 2012, pp. 597-611.
- Deanna Caputo, Shari Lawrence Pfleeger, Jesse Freeman and M. Eric Johnson, "Going Spear Phishing: Exploring Embedded Training and Awareness," IEEE Security & Privacy, 12(1), January 2014, pp. 28-38.
- Deborah Mayo and Rachelle Hollander, Acceptable Evidence : Science and Values in Risk Management, Oxford University, Press, 1991

HOW TO ASSESS – NON LOCATIONAL

- Human resources issues
  - Don't do this yourself, use HR!!
  - This applies to everything else!!!
  - *You DO have allies!!!!*

JUST THE BEGINNING!!!

In the previous I have only scratched the surface!!!

Don't try to do all of this yourself (your could hire me…but remember you have experts in your own organization, bust those silos)

Bring everyone in and you will be on your way to real Cyber-resilience

QUESTIONS?
COMMENTS?