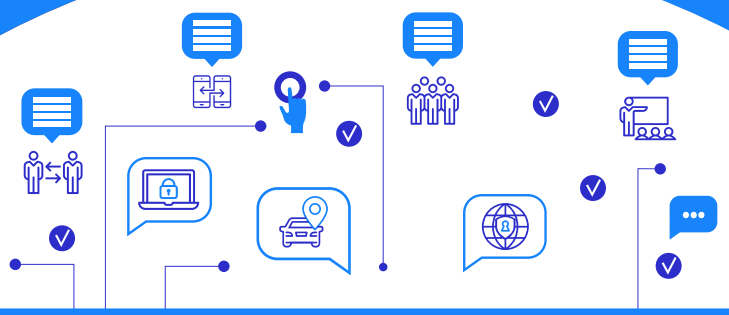
Security for the Hyperconnected World

WILLIE APPEL
Founder of DigitalMindz



EMPOWERING THE SECURELY CONNECTED WORKFORCE

BlackBerry® Secure™

WORLD TOUR

Security in the Hyperconnected World

ABUNDANCE NEEDS MACGUYVER

Willie Appel
Founder – DigitalMindz
12 June 2018

ABUNDANCE NEEDS MACGUYVER

MACGUYVER AS A VERB AND NOT A NOUN

- MacGuyver was Series now a verb, right?
  - Yes, it means to fix, adjust or make something using whatever items are at hand, to improvise a solution to a problem using minimum material, maximum scientific knowledge.
- In *Abundance,* Peter Diamandis & Steven Kotler, holds MacGuyver up as a DIY model –
  - *What would MacGuyver do?*
  - Empty his pockets and get the job done with a role of Scotch tape, paper-napkin, and a paper clip…

THE HYPERCONNECTED WORLD

SOFTWARE IS ***STILL*** EATING THE WORLD

- Marc Andreessen – penned this quoted in the WSJ Aug 2011 (Italics – Willie).
- Today the idea that ***"Every company should be a software company"*** is almost a cliché.
- Marc today:
  - "Six decades into the computer revolution, four decades since the invention of the microprocessor, and two decades into the rise of the modern Internet, all of the technology required to transform industries through software finally works and can be widely delivered at global scale."

- ***Sine qua non:*** **It's not about what can we do now. It's about what can we do now, that was simply not possible until today! Are you ready to re-imagine your business, or disrupt your industry? It's a discontinuous leap — supported by the rise of new platforms, and with it the rise of new security challenges. ARE YOU READY?**

THE NUMBERS ARE NO LYING – SECURITY IS RISK AT SCALE

The Mirai botnet that hit in late 2016 demonstrated how hackers can use a botnet army of compromised IoT devices to launch a massive DDoS attack. IoT-based attacks will likely continue to grow in 2018, including those on both devices and cloud backplanes, as hackers try to compromise systems for ransom or to steal sensitive information.

Mirai was simple hacking, it checked for open doors, IoT Troop or Reaper is actively picking locks, and has already found access to more than 1 mil networks and counting – The REAPER is coming!!

By 2020, 100% of large enterprises will be asked to report to their boards of directors on cybersecurity and technology risk at least annually, which is up from today's 40%.

By 2020, 60% of Digital Businesses Will Suffer Major Service Failures Due to the Inability of IT Security Teams to Manage Digital Risk.

Gartner

Source: Gartner

The now for the Scary part –

1. More than 95% of all ATMs are still running Windows XP (13 years old and not supported by Microsoft)!
2. Your DVR in your house/office, connected to your WiFi, is running an even older version of OS software, and
3. So is the router you received from you trusted Internet service provider, or not, so you downloaded the latest set of patches?
4. Or a simple factory reset will do the trick – at least it kills malware ☺

51%
of transactions in the Network come from mobile devices.

60%
of all account creations come from a mobile device.

1 Billion
bot attacks this quarter.

Source: Threatmatrix 2018

SECURITY IN A HYPERCONNECTED WORLD

BILL SCHNEIER – SECURITY GURU - SAYS

- In this Cyber-physical world, everything is a computer – we started with things, then we had things with a computer in them, and now we have computers that do things – like driving cars!!
- Security is our collective responsibility, but we need help.
- We need to develop a common set of expectations to address risks, and to define the roles and duties of all participants in the digital ecosystem.
- This obligation encompass several issues – from privacy norms to cyber governance to government participation –our ability to manage risks is the crux of cyber resilience.
- As the risk of cyber-attacks becomes more prevalent, the cost of attacks to the public, institutions, economy and society is growing.
- ***Sine qua non:*** **To be able to continue to reap the positive benefits of innovation and technological developments, we need a new paradigm of security in this hyperconnected world.** ***Willie: How about a United Nations body for Cyber Security & Risk?***

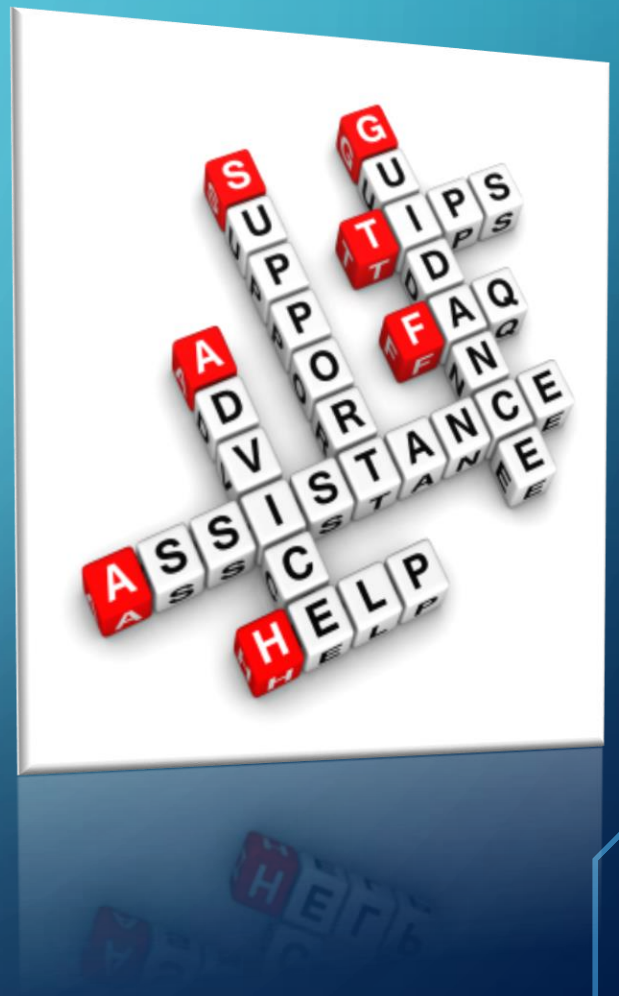
WE ARE ALL ENGINEERS, AND…

- We are building a robot the size of the universe – not just a Star Wars robot,
- A real distributed robot, not designed, but emergent, evolving, AND
- It has and will have significant impact on the security systems of our world.
- Why, because we (the Collective Commons[1]) are all contributing to it, and it is on a tight cycle and steep learning curve.
- ***Sine qua non:*** **Internet/Cyber security becomes everything security – security expertise is now available every where,, but so is the threat. The CIA triad – Confidentiality, Integrity and Availability is under attack, specifically the last two – hack my computer and I loose some data, hack my car's braking system and I loose my life – It is catastrophic**

1. Jeremy Rifkin – The Zero Margin Cost Society

HELP IS COMING – ARE YOU CONNECTED

- Regulators are starting to step in, protecting personal data (GDPR) and critical infrastructure.
- Industries are beginning to issue best practices and to collaborate on incident response.
- Policymakers (in EU) are waking up to the need to upgrade our legal frameworks.
- Technologists are also starting to tackle the modernization of an infrastructure designed for openness, not security.
- A number of real end-point technology specialist companies are putting their hands up when it comes to a holistic understanding of the security needs of the modern enterprise.
- ***Sine qua non:*** **Big change is needed; governments needs to be involved – we are used to a regulated world – banking insurance, etc… but we do not have a regulatory system that holistically can handle security – governments but also software still likes silos, regulatory bodies are all separated – a new governance body is required to regulate The Threat, and it needs to happen before somebody dies – fear makes governments move - think 911.**



IT IS MORE THAN AN ARMS RACE, IT IS A "**HOW SAFE AM I**" RACE AND YOU NEED A PARTNER

- One of the leaders of the Gartner MQ for EMM Suites - 2017
- In Dec 2016 released BUEM - Blackberry Unified Endpoint Management – managing all user end-points including IoT devices, all combined now in BEMS – Blackberry Enterprise Mobility Suite.
- The number one provider of Personal Information Management (PIM)
- The combined history, reputations and security capabilities of BlackBerry, WatchDox and Good Technology make BlackBerry a strong choice for regulated or security-conscious organizations.
- ***Sine qua non:*** **Have you already Blackberryed your security environment and IoT eco-systems? Now is not to late!**

BOTTOM-LINE: BUILD STRONG CYBER RESILIENCY[1]

- The cyber resilient business combines the capabilities of cybersecurity, business continuity and enterprise resilience into a governed set of tactics.
- It applies fluid security strategies to respond quickly to threats, minimizing the damage and continue to operate under attack.
- The result, a cyber-resilient business which continues to introduce innovative offerings and business models securely, strengthen customer trust, and grow with confidence.

Source: 1. Accenture Security – Gaining ground on the cyber attacker – 2018 State of Cyber Resilience

KEEP CALM AND THANKS FOR LISTENING