RETHINKING ENTERPRISE SECURITY

G. Huntington

President,

Huntington Ventures Ltd.

March 5, 2022

What This Deck Contains…

- A review of rapidly emerging new attack vectors
- Rethinking human and AI system/bot identities
- Rethinking IAM infrastructure leveraging graph databases
- Leveraging TODA rethinking centralized/decentralized security
- Protecting your enterprise from tech used in behavior predicting
- Rethinking use of biometrics
- Creating secure infrastructure allowing your enterprise to begin to edge into the metaverse type environments
- Creating a new security model which updates every second protecting your enterprise from IoT, bots et al

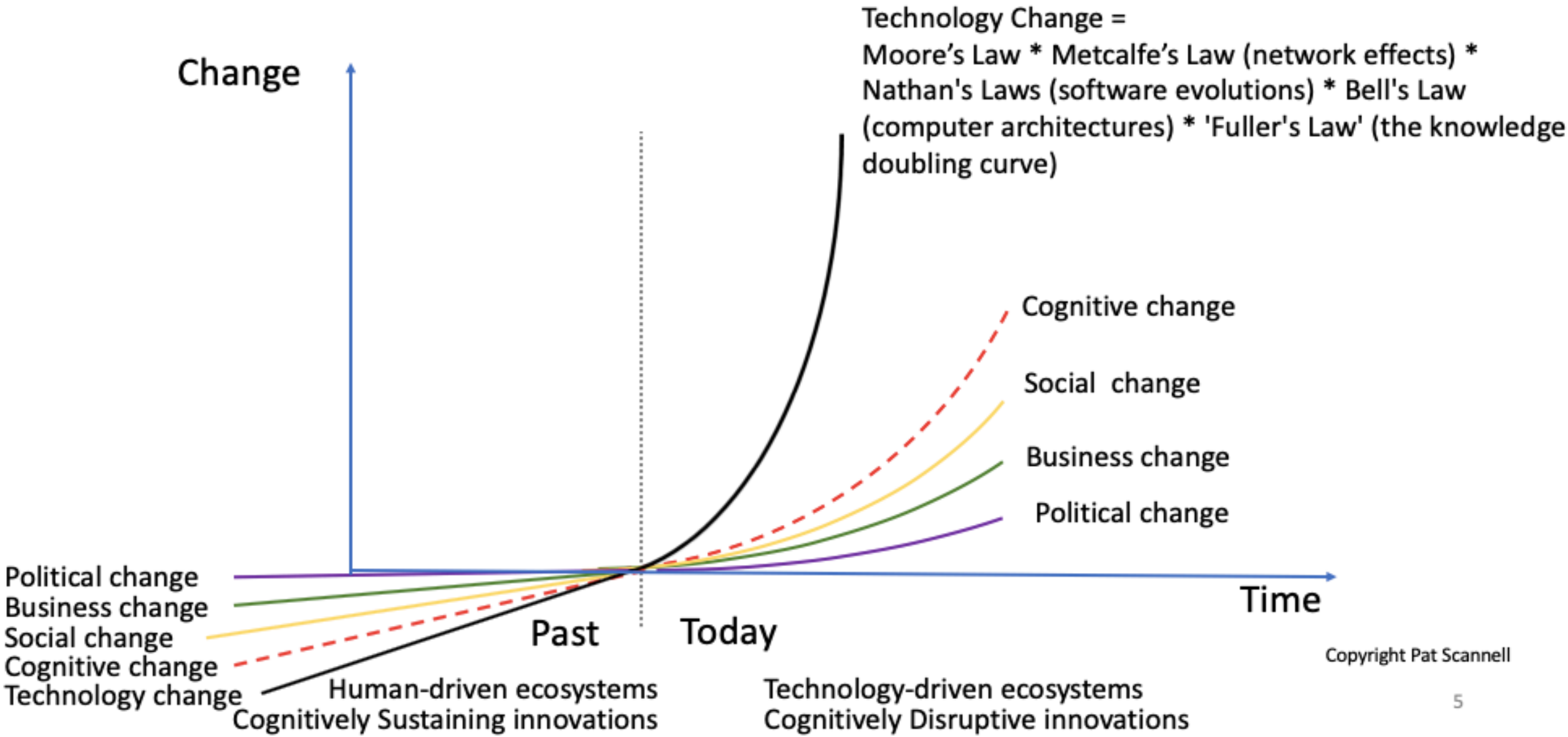
Review These Enterprise Decks…

- "The Sky Isn't Falling – But Security Models Must Change"
- "Rethinking HR Practices"
- "Marketing Risks In A New Age"
- "Changes in Enterprise Legal Departments"
- "Securing Manufacturing"

Rapidly Changing Threat Landscape

- The decks all refer to a rapidly changing threat landscape
- At the 100,000-foot level it's composed of:
  - Behavioral tech
  - AI systems and bots, both physical and digital
  - Rapidly emerging smart digital identities of us
  - IoT devices
  - AI/AR/VR environments
- All merging together, leveraging connectivity, to create what was once thought of as science fiction when I was growing up
- It's created by this curve…

How Fast Will Disruption Happen?



My Premises:

- The tech isn't just emerging, but it's also merging, rapidly creating new attack vectors
- Our existing IAM and security vendor suites aren't able to keep up with the changes
- New attack vectors created by behavioral/recording tech, bots et al opens up new doors to attack sensitive enterprise assets and digital content
- A rethought enterprise security model is required, which is updated each second based on risk

As You'll See From the Aforementioned Decks

- I'm not just talking about security "vision" type stuff i.e., the models
- Down in the operational weeds, I'm also talking about small baby steps your enterprise can take to get itself positioned for this revolution we're living in
- Like what?

Leveraging Wireless Free Areas

- The Malicious Molly and Jane Doe story in the HR deck, illustrates the invasion of behavioral predicting tech as well as leveraging AI
- Depending on risk, your enterprise should consider creating wireless free areas where high risk interviews, negotiations et al can occur
- It's a first step to thwart malicious folks, criminals and Evil Inc. mitigating some of the risks from leveraging this tech to attack your enterprise

LDAP

- In the 90's, as the identity industry began, enterprises IT rapidly adopted a protocol called LDAP (lightweight directory access protocol) because it was lightening fast to integrate authoritative HRMS systems to and then point all other enterprise apps to it about the identity
- As SSO and authorization evolved, IAM systems were built on top of it
- However, it has one drawback…its architecture
- It uses a tree shaped structure which means establishing a many to many or many to one relationship between identities doesn't work well

Enter Graphs

- I have a friend, Derek Small, who's company, Nulli, for the last several years has been pioneering use of graphs to replace LDAP identity data stores
- They've successfully deployed it with several large enterprises
- I strongly suggest you contact Derek or, ask me to provide you with an introduction

Graph Premise

- Graphs will replace LDAP as the core of IAM systems for identity data
- This enables fast changing, potentially complex identity relationships to occur between human physical identities and their smart digital identities, IoT devices, AI systems and bots, both physical and digital

TODA

- As the other decks state, I don't like blockchain and went looking for a better solution
- Skim this article "Legal Identity & TODA"
- So, as the other decks state, the place to begin is by rapidly doing POC's and pilots to learn what works in your enterprise and what doesn't work
- TODA files and capability files can be strongly leveraged in your enterprise identity architecture

Centralized/Decentralized Security Architecture

- Skim this article, "Part IV – Toda Based Decentralized Enterprise Authentication and Authorization"
- It proposes leveraging TODA, and TODA capability files to create the beginnings of a new centralized/decentralized identity architecture
- It also offers enterprises the possibility of creating delegate-able authorization rights which may or may not be time based

Biometrics – I Hate How They're Used Today

- Skim this article, "I Hate How We Use Biometrics Today"
- If a malicious person or Evil Inc. gains access to them, we're screwed for many years i.e.,
- THEY'RE NOT REVOCABLE AND RESISSUABLE
- So, in the marketing deck I propose some ideas you folks might want to ponder and do some research on…

Rethinking Biometrics Within Your Enterprise

- Consider offering your customers a service where they voluntarily offer their biometrics, which you then either digitize and/or anonymize, digitally signing them
- Issue them back to your customer in a TODA file which they then control
- So, depending on risk, they'd potentially use their biometrics to verify their identity
- You'd compare the digital signature on it to the one you signed – If it's still valid, then you'd have a high degree of assurance it's say Jane Doe
- If the biometrics are maliciously obtained, the customer would come to you, prove their identity, you'd then revoke the old biometrics, and reissue new ones
- This is much better than the existing crappy systems we use today for biometrics

Now, Is This Easy To Do - NO

- So, don't think you can easily do this in the next few months
- My point?
- The first companies that figure out how to do this will be able to offer their customers a way where they keep control of their biometrics and, if they're stolen, easily be able to revoke and re-issue them
- It's a large revenue generating idea with associated risks
- Which is why, I'm proposing that banks and insurance companies, who are facing increased marketing pressure, are possible partners to do this

Then There's AI Systems and Bots…

- To see what's rapidly coming at you skim these articles:
- "Why AI Regulation Requires Legal Identities of AI Systems and Bots"
- "Artificial Intelligence & Legal Identification – A Thought Paper"
- "Mission Control – We Have a Problem"
- "Lease or Rent a Bot! Rapidly Emerging Contract Law & Legal Identity Challenges"
- "Nanobots & Legal Identity"
- "Micro Flying Bots & Legal Identity"
- "Microbots Able to Swim Through Your Body & Legal Identity"
- "Bots, Swarms, Risk & Legal Identity"
- "Nanobots, Microbots, Manufacturing, Risk, Legal Identity & Contracts"

AI System and Bot Identities

- The existing legal identity architecture for AI Systems and Bots doesn't exist on the planet today
- So, as the other decks state, I've developed an architecture for this:
  - Humans:
  - "Rethinking Human Legal Identity"
  - AI Systems/Bots:
  - "Creating AI Systems/Bots Legal Identity Framework"
- **BUT, until jurisdictions implement it, it's not going to help you in the short term**
- Given this, what can you do?

Proprietary Solutions...

- There isn't one nice neat answer to this
- Instead, here's my thoughts to you IT Security folks on possibilities..

Physical Bots

- As your enterprise either buys, rents, leases, or leverages bot services via contracts with suppliers, depending on risk, here's your alternatives..
- Leverage existing manufacturer bot ids
  - This works well in situations like running a 2,300 physical bot hive
  - It might also work well for situations like this outdoors, where the service is run by another
- However, it all depends on not only your security risk, but also legal risk
- So, one thing you, Legal, HR, Marketing and Manufacturing can do together is to develop policies for identifying bots and IoT devices within your enterprise

Digital Bots

- This is a much harder problem to solve – why?
- Depending on risk, the bots might require a very solid identity which is tamper proof by criminals and entities like Evil Inc.
- So, you folks should begin pondering how you're going to solve this in-house or, via associations or, via vendors
- The bottom line is a unique identifier MUST be written to the underlying source code in such a way it's VERY secure
- Additionally, ports will likely need to be specified to quickly access and determine a bot's identity

Here's The Challenge…

- Digital bots can be created at speeds of hundreds of thousands or more per second in one jurisdiction on the planet and, in the next instant, be operating in all other jurisdictions, potentially masquerading as another and/or attacking your enterprise
- My point? Your existing security strategy isn't likely going to hold up well without a secure means of instantly determining friend from foe

Different Bot Identity Assurance Levels

- So, based on risk, you're going to likely require creating different levels of bot identity assurance for a given bot
- Currently, there's been very little thought about this on the planet

As AI/AR/VR Emerges, Risk Rises

- Skim these articles:
- "Metaverse Bots? "
- "Lifelike Avatars, Risk & Legal Identity"
- "Metaverse, Identity, Data, Privacy, Consent & Security"
- "Challenges With Metaverse Contracts"

So, It's In Your Own Interests…

- To begin lobbying jurisdictions in which you operate to get their political rear ends in gear to create a global/local AI system and bot legal identity architecture…
- As well as a human one – why?
- You need to instantly be able to determine if it's a human or a bot you're dealing with
- This is especially true as AI/AR/VR "metaverse" like environments emerge
- This is the desired mid to long term solution

Let's Assume It's NOT Going to Quickly Happen

- The slowest rate of change in this curve is political
- Thus, waiting for politicians to "do their stuff" isn't a viable solution
- So, in some of the other decks I created a story to use as a use case for your enterprise
- It leverages your new age IAM infrastructure leveraging graphs and TODA, along with your ability to assign unique identifiers to physical and digital bots of many different types
- I'll display it here again…

Your Customer Jane Doe Et Al…

- Jane Doe creates smart digital identities for herself, her partner Sally Smith, and for her son John
- Your CRM system specifies how these smart digital identities can be verified, writing a TODA capability file to each smart digital identity's source code
- The type of relationship is specified by the CRM and written to your enterprise's underlying graph database i.e., your IAM architecture

You Can Tailor Services For Them

- You might offer Jane or Sally the ability to specify what John can or can't do with your enterprise
- This might or might not be the same for John's smart digital identity
- Jane and Sally for example might be able to specify a dollar range John can use with you
- They also can hypothetically attach a time-based limit to John's abilities to spend
- Yet there's more you can do…

Add Bots To the Relationships

- So, if Jane, Sally or John buy or lease physical or virtual bots, you can leverage your CRM/TODA/Graph infrastructure to quickly add different entities to your enterprise relationship
- You can also allow them to tailor what these entities can and can’t do with your enterprise via TODA capability files
- As these types of entities come and go, the infrastructure allows you to keep it all organized, secure and mitigate risk

Metaverse Services

- So, if Jane, Sally or John interact with your enterprise via a “metaverse” type environment, it’s now no big deal
- You can identify the entities presenting themselves to you as Jane’s, Sally’s or John’s avatars etc.,
- Based on risk, ask them to increasingly verify themselves, and do business with them
- This is the stuff the “metaverse folks” aren’t talking about today

Security Models Aren't Going to Work Well

Why?

Risk Changes Moment By Moment

Enterprise and personal risk rapidly increases, from moment to moment

Over time, not over night, our old security models now will no longer work well

It requires a bottom up, second by second, risk assessment of many interlocking variables

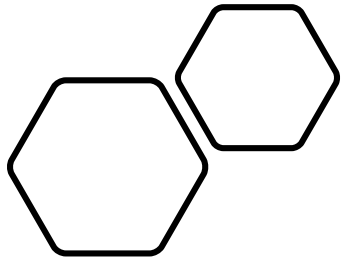
Thus, I've created, at the 100,000-foot level a new security model…

Zones of Trust

It's Dynamic, Assessing Risk/Trust Per Second

- In this article, "Smart Cities - Contracts, Privacy, Data & Legal Identities", I discuss you walking down a street in the not-so-distant future wearing AI/AR glasses/contact lenses and smart clothes with IoT devices embedded within them
- **Thus, you're in the physical and virtual world at the same time**
- This is a mind shift most people haven't yet realized

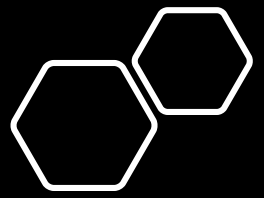
It’s Dynamic, Assessing Risk/Trust, Second by Second



- Around you there’ll be LOTS of increasingly smart IoT devices
- People walking towards you wearing the same tech
- AND LOTS OF BOTS BOTH PHYSICAL AND DIGITAL
- **This changes the risk game since all of this is, what I call in my head, one whopper sized data capture, behavioral predicting environment about you**

It's Dynamic, Assessing Risk/Trust, Second by Second

- Watch this video and pay attention just after the 1:00 minute mark
- All those people walking towards you and buildings you cycle by will easily be able to identify you, predict your behavior et al
- **It throws into the dustbins of time our old ideas of privacy**



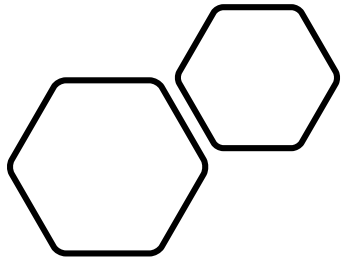
Three Premises…

Each of us needs a new security/privacy model, tools and laws/regs giving us the option, if we choose, to live privately in a very non-private world

Enterprises MUST change their risk/trust frameworks to begin getting ready for this

Putting it bluntly – it's damned hard to do today because we lack toolkits of tech, laws/regs and contracts to easily meet the challenges

To Learn More About the Models…



- Skim these two articles:
- "New Physical/Cybersecurity Security Model"
- "Smart Cities - Contracts, Privacy, Data & Legal Identities"

Down In Reality Weeds...

What baby steps can your enterprise take to work towards creating the model?

Step 1: Rethink Your Existing Security Zones

- You need to do this through the lens of people, bots, and things, having an increasing array of sensors leveraging IoT devices, penetrating your security zones, with malicious intent
- This means old traditional zones won't work when the person enters the physical/digital trust zone

Step 2: Begin Creating PIAMS for Key People

- Key people within your enterprise now require their own enterprise PIAM (Personal Identity Access Management) system which protects the enterprise second-to-second – Consider Jane Doe an exec…
- She gets up at home and enters the enterprise metaverse type environment to work
- She then gets in her car and drives to work or wherever but around her and her car are LOTS of IoT devices, bots et al, as she talks to clients negotiating a deal
- She then walks through your physical facilities to your most sensitive zones
- All of the above now requires second-by-second analysis of enterprise risk and then implementing trust mitigating the risk

Step 3: Encourage Implementation of the New Human and AI System Bot Architecture

- If you're a small to medium enterprise, you frankly don't have the resources to properly address what this deck talks about
- Thus, it's in your best interests to lobby your local and national politicians to implement the new architecture this deck references
- This then gives you not only the ability to determine people and bots legal identities but…
- It also gives your personal PIAM to interface with
- Hypothetically, in the future, you can leverage this as part of your enterprise security strategy

Step 4: Research on How To Detect IoT Devices

- Come with me into the not-so-distant future when a person and enterprise are surrounded by thousands of increasingly smart nano and micro sized IoT devices
- THEY WILL BE MALICOUSLY USED
- So, Evil Inc. won't care about laws and regs, and will leverage these to the hilt as attack vector tools
- One big question that's been in my mind for the last few years, for which I don't have an answer to, is how an enterprise or person can detect these malicious devices when they're not playing by the rules?

You Likely Need To Partner Up…

- If you don’t have whopper sized research budgets, you’re going to likely need to partner up with others to rapidly work towards answering the question

The World Is Changing…

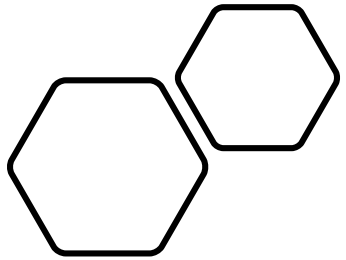
- This curve means the rapid pace of change continually increases, thus also increasing enterprise legal risk
- So, rather than wait for “bad things” to happen within your enterprise and knee-jerk to it, you folks should be meeting monthly with your Legal HR, Marketing and Manufacturing teams to alert you to new risks
- These are “out of the box times” requiring “out of the box” thinking

This Is The Future Madly Coming At You

So, you can be like the turtle slowly lumbering down the road, potentially being run over by criminals, malicious competitors et al…

Or, you can be like the hare, ready to nimbly move, taking advantage of the tech change, while mitigating your risks

My Favorite Quotes



We cannot solve our problems with the same thinking we used when we created them” – Albert Einstein

“Change is hard at first, messy in the middle and gorgeous at the end.” – Robin Sharma

“Change is the law of life. And those who look only to the past or present are certain to miss the future” – John F. Kennedy

About Guy Huntington

- I'm an old, very experienced, identity architect whose past clients include Boeing, Capital One and the Gov't of Alberta's Digital Citizen Identity & Authentication project
- I've spent the last six years working my way through and creating a new legal identity architecture for both humans and AI systems/bots and then leveraged this to rethink learning
- I'm currently aggressively fund raising $5-10 billion to do this in 1-3 jurisdictions on the planet
- In the meantime, I'm doing short term C-suite consulting assisting enterprises to get them ready for the revolution this deck and others talks about

To Learn More About Me...

- Skim these articles and read the extensive reference links at the end:
- “An Identity Day in the Life of Jane Doe”
- “Revised Principles of Identity”
- “I Hate How We Use Biometrics Today”
- “DIGITAL IDENTITY...”
- “The Times They Are A-Changin'”
- “Digital Transformation Requires Change to Our Old Ways of Doing Things”

Contact Information:

- Guy Huntington
- President, Huntington Ventures Ltd.
- LinkedIn: https://ca.linkedin.com/in/ghuntington
- Web: https://hvl.net/
- Email: guy@hvl.net
- Phone: 1-780-289-2776
- I live in West Vancouver, BC, Canada

Appendix: - Legal Identity Architecture

- **Humans:**
  - “Rethinking Human Legal Identity”
- **AI Systems/Bots:**
  - “Creating AI Systems/Bots Legal Identity Framework”

Appendix: - Learning Architecture

- “Learning Vision Flyover”