SECURING MANUFACTURING

G. Huntington
President,
Huntington Ventures Ltd
March 8, 2022

What This Deck Contains

- Identification of rapidly emerging risks to manufacturing from criminals leveraging new tech
- Suggested small baby steps to take towards addressing them

I'm NOT A Manufacturing Expert…

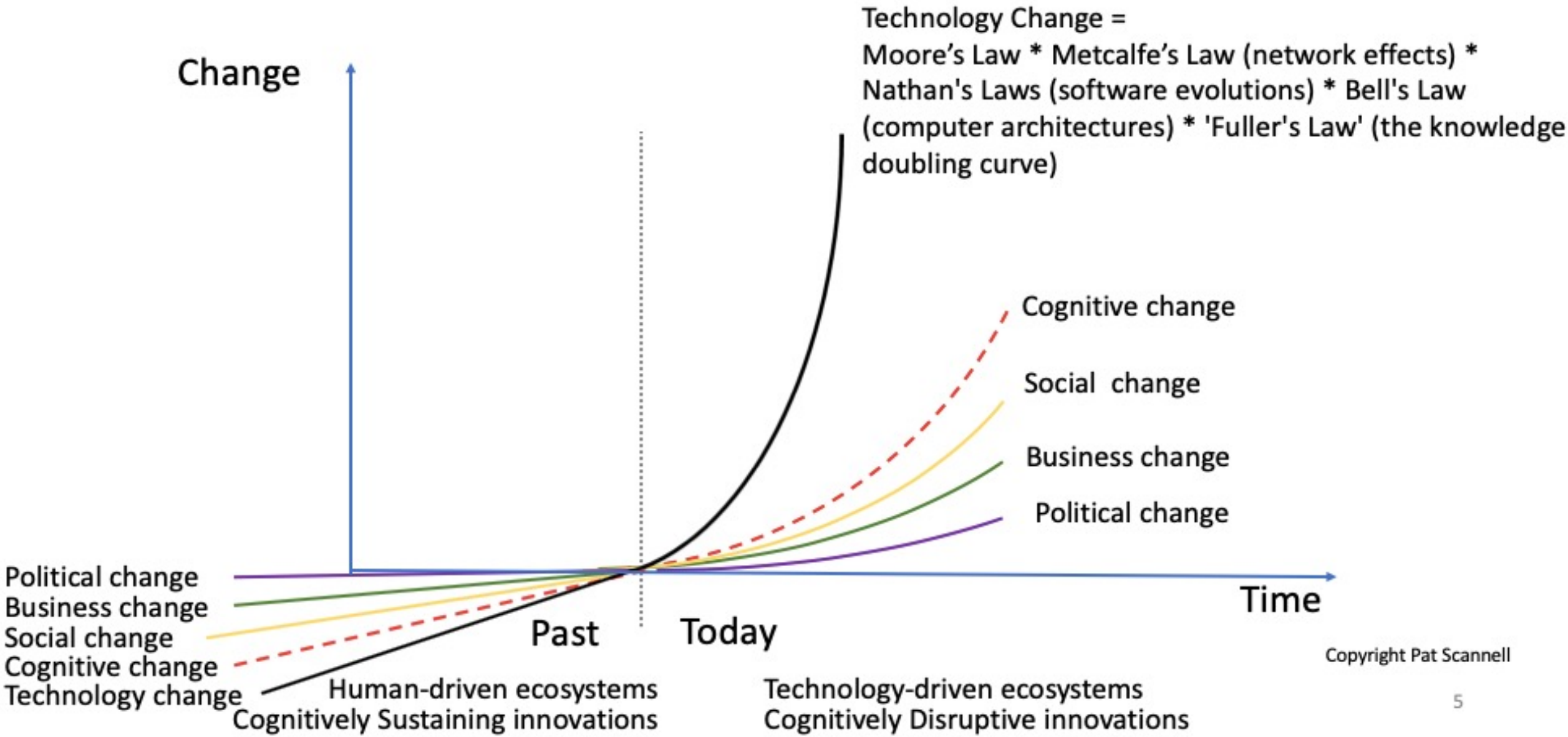
- I have worked with some SCADA systems
- For example, I was the identity architect many years ago for a utility. I convinced the CIO to bring in some folks to attack the utility. Within an hour after landing, they were able to take control of the grid from their laptop, which resulted in an immediate security project
- But the point I want to make upfront is I haven't worked with manufacturing processes and security
- So, why listen to me?

I'm An Out of the Box Thinker In Out Of The Box Times...

- My focus has been on identities, starting with human ones, both physical and digital
- It then progressed to AI system and bots' identities
- From there it's progressed into IoT devices
- All of which is making its way into manufacturing processes

It Starts With This Curve...

How Fast Will Disruption Happen?



Copyright Pat Scannell

My Premises

- Increasingly complicated manufacturing systems, are increasingly digitally linked to supply chains
- The tech change curve not only allows for new ways of manufacturing, BUT IT ALSO CREATES ALL SORTS OF NEW ATTACK VECTORS
- That's what this deck dives into...

Skim This Deck…

- "**The Sky Isn't Falling – But Security Models Must Change**"
- Read the section on Acme Inc. and their sensitive, manufacturing process
- Then read the two slides discussing Toyota's recent shutdown in Japan from a cyber-attack

All Sorts Of New Attack Vectors

- Physical bots:
- Now are flying microbots easily usable today?
- No – why I used it was to show the tech is now here, in a crude way, to hypothetically use it maliciously
- Thus, rather than wait to be successfully attacked by it, enterprises, where the risk levels are high, should begin pondering measures of how to mitigate the risk

A Physical Bot Isn't Just a Bot

- The rise of fast emerging sensors and nanotype tech is shrinking down these to very small devices
- They can easily be inserted into other bots
- For example, if your company is using bots to clean floors etc., then these become possible attack vectors
- They can be equipped with many sensors and/or used to release micro and nonbots into your environment

Do All Bots Require Legal Identities?

- No. It depends on risk
- So, **this 2,300 physical bot swarm** likely can use the manufacturer ID's to identify them since they're contained within a facility
- HOWEVER, where risk rises and bots interact outside or in multiple facilities, then legal identity will be required

Then There's Virtual Bots...

- These are rapidly morphing into "smart bots" able to do increasingly complex tasks, deal with emotions, etc.
- They can be created by an AI system at awesome speeds i.e., hundreds of thousands, or more per second

Do They Require Legal Identities?

- It depends on risk
- So, hypothetically let's say your process engineer Jane Doe has a smart digital identity of her, which can multitask, interfacing with segments of your manufacturing processes, as well as with physical and digital bots
- Now her legal identity, for not only herself but also for her smart digital identity, becomes likely required

Evil Inc.

- Will leverage all sorts of different attack vectors to effectively “worm their way” into the heart of your process control operators and systems
- They’ll be looking to masquerade as them, or worse shut down your production systems
- They’ll also be looking at your process sensors, devices et al looking for weaknesses…

Smart Devices, Sensors, Pumps Et AL

- In any industrial process there are likely hundreds, thousands, or tens of thousands of sensors monitoring the process
- Then there's all the different pumps, machines et al
- Typically, they're controlled by a process control system

They're Extremely Insecure

- Today on the planet there's no global standards for:
  - Legal identity of them (relies on manufacturer provided identities)
  - Authentication standards
  - Authorization standards
  - Security best practices for the sensors, devices, et al

Which Increases Risk

- The Evil Inc.'s of the planet thus have LOTS of potential attack vectors to use against this
- My point?
- Given **this curve**, it means your enterprise processes become, over time, not overnight, increasingly vulnerable to attack, ransomware, etc.

It’s Damned Hard To Solve…

- Why?
- Sensor and device suppliers are global
- There’s also grey market suppliers
- Further, some machines et al are a composite of different supplier parts
- There are literally hundreds of millions or billions of old devices et al already installed around the planet

I DON'T Have a Magic Wand...

- To wave that instantly solves this
- However, I'm on the hunt around the planet for companies and jurisdictions who want to solve this by creating standards for identity, authentication and security for sensors, machines et al
- Contact me if you're one of them

A Future Vision Story

- Let's say your manufacturing process leverages emerging smart electro-mechanical pumps
- Depending on risk, you might accept the pump manufacturer's ID as Pump 12345
- Or you might want to assign it your own identity your process control system uses as Pump ABCDE

A Future Vision...

- Let's assume you agree to give Pump ABCDE certain authorization rights pertaining to flow per second ranges
- Now let's assume that an emergency condition arises where you want to dramatically change Pump ABCDE's operating conditions
- Your process system, and/or operator like Jane Doe, might have to instantly authenticate themselves to Pump ABCDE, as well as Pump ABCDE authenticating and authorizing itself to them using pre-agreed codes or whatever
- All of which are new potential attack vectors

Malicious Molly Attacks

- You folks also need to sit back and contemplate what a Malicious Molly can do, if she successfully penetrates your facility as an employee, contractor, etc.
- She might be wearing clothes et al which have an increasing array of sensors
- So, the question you need to be asking is what kind of data can she obtain which would be damaging?
- Then design risk mitigation strategies

Supply Chain Attacks…

- If your manufacturing processes are tightly integrated with suppliers, just like Toyota, then it's possible to attack you via another part of the supply chain
- My Point?
- The curve is generating all sorts of new attack vectors such that you shouldn't rest on your laurels after securing the interlocking processes

Operator Identities...

- You should have already implemented an authentication/authorization structure based on risk
- So as risk rises, you should be requiring additional information it's really the process operator, or the process system
- If you're using biometrics as part of this...

I Hate How We Use Biometrics...

- Skim this article "**I Hate How We Use Biometrics Today**"
- So, what happens if Evil Inc. gains access to your operator's biometrics?
- Rather than just relying upon "Liveliness Tests", it might be worth your while to consider implementing your own biometric scheme where you digitally sign them

Wireless Areas…

- One of my recommendations to HR et al is to think about creating wireless areas within your enterprise where the Malicious Molly tech won't work
- This might be a stupid idea for your manufacturing areas or, a good one
- However, I put it out there as an idea for you folks to mull over

Security Zones...

- In the deck referenced earlier, I'm proposing rethinking zones of trust/risk
- It references this diagram...

Zones of Trust

Risk Changes By The Second

- I'm not saying the sky is falling and you folks should become paranoid about security each second
- HOWEVER, what I am saying is, depending on risk, high risk scenarios need to be rethought
- You need to view this through the lens of Evil Inc. who's going to leverage all the tools they can to crack your defenses

Evaluate Based on Risk From:

- Physical
- Digital
- Humans (Physical/Digital)
- AI Systems/Bots (Physical/Digital)
- IoT
- Metaverse

Identity Relationships…

- In your world, you likely have hundreds, thousands or more of devices, machines, controllers, et al
- My point?
- The arrival of increasingly smart IoT plus bots, both physical and virtual means your identity relationships between each of these will likely grow

Enter Graph Databases

- **In the deck referenced earlier**, I suggest a baby step is to implement graph databases within your enterprise
- It applies to you folks in manufacturing as well
- As the types of devices, controllers et al rapidly grows, so to will the need to establish identity, authentication and authorization relationships between them

TODA…

- **The deck referenced** also discusses TODA - Skim "**Toda Primer**" and "**Legal Identity & TODA**"
- It likely applies to you folks in manufacturing as well
- As process control commands et al are now sent between different supply chain systems they'll require security

TODA Over IP...

- Enables you folks to be assured Command 1 actually happened securely
- So, Device 12345 exists in Enterprise 1 and Device ABCDE exists in Enterprise 2 can now securely communicated such that Command 1 was sent from Device 12345 to Device ABCDE on such a date, at such a time, also containing a hash of the command

Authorization Rights…

- Hypothetically, Device 12345 could pass a TODA capability file from Enterprise 1 to Device ABCDE in Enterprise 2
- The capability file hypothetically could contain authorization rights

It’s Not Ready For Prime Time

- **As the deck states**, this needs to be POC’d and piloted
- If you’re interested, contact me

Digital Twins and Metaverse

- Manufacturing has been leading the way with use of digital twins
- My point?
- As the “metaverse” expands, depending on risk, then identities within it require at the least industrial strength identification and likely legal identification

Which Doesn't Exist Yet

- Thus, as supply chain type systems become "metaverse entwined", then your risk rises
- My dumb question to you folks is how will you identify these types of entities?

Identifying Digital Entities…

- Requires the ability to write to the digital entities source code unique identifiers which can’t be manipulated by Evil Inc.
- It also requires the ability to query specific ports to rapidly confirm the entity’s identity

Different Strengths

- Further, depending on risk, it also requires the ability to have different identity and credential assurance strength levels
- All of this is mostly NOT BEING TALKED ABOUT TODAY!!!!!!!!

So, It's In Your Best Interests...

- Lobby jurisdictional leaders where you operate to get their collective rear-ends in gear to fund and implement new legal identity architecture for both humans as well as AI systems and bots (see appendix slide)
- Then you can leverage this to strengthen your security models with

YES, IT'S VERY COMPLICATED!

- There isn't a nice neat solution which solves all the aforementioned areas
- Thus, you need to work with IT security, Legal et al to mitigate the risks

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 any of these articles and 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’”**
- “The Sky Isn’t Falling – But Security Models Must Change”

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: Enterprise Decks

Appendix: Legal Identity Architecture

- **Humans** - "Rethinking Human Legal Identity"
- **AI Systems/Bots** - "Creating AI Systems/Bots Legal Identity Framework"