



# Cyber Security, Crime and Global Trade

TAPA T1 Virtual Conference

Thursday June 17<sup>th</sup>, 2021

Pete Mento, Mento LLC



# The rail ecosystem (a partial view)

## Train tracking & speed monitoring

Location and speed monitoring by GPS, cellular triangulation, and other telemetry sources.



## Automation systems and Vital system control

Positive train control (PTC), communications-based train control (CBTC), automatic train supervision (ATS), safety-critical systems, operationally-critical systems



**Wayside equipment**  
Signals and switches, wayside interface switch equipment, etc



**On-Board Systems and cab display**  
Locomotive control, passenger comfort systems, environmental control, industrial control systems, communications equipment, automation and more

**Convergent Infrastructure**  
Shared, data, and analyticscommodity IT infrastructure, resourcing – or support OT functions



**Distributed Control**  
Dispatch, operations control centre (OCC), maintenance yards, communications and control systems, signalling, radio communications, etc.

**Information Systems**  
applications to manage final product delivery, logistics, human resources, and ticketing


**Train, Track, & Yard Management**  
Supporting data-related systems and infrastructure for all of the OT/IACS assets currently in use.

**Wireless Networks**  
Asset tracking, personnel safety wearables, logistic tagging & monitoring, localized private connectivity, passenger connectivity



# Glad the Politicians are all over this....

- Last month, the US and the UN drafted a listing of agreements everyone will work from regarding cyber attacks and cyber crimes.
- They are virtually IDENTICAL to the same standards they drafted and ADOPTED in 2015.



“Another area we spent a great deal of time on was cyber and cybersecurity. I talked about the proposition that certain critical infrastructure should be off limits to attack — period — by cyber or any other means. I gave them a list, if I’m not mistaken — I don’t have it in front of me — 16 specific entities; 16 defined as critical infrastructure under U.S. policy, from the energy sector to our water systems.”

President Joe Biden (possibly the dumbest remarks ever made publicly by a sitting president regarding cyber security) June 16<sup>th</sup>, 2021



# Don't worry Mr. President, I'm on it.

- There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.
- Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure..

# CRITICAL INFRASTRUCTURE SECTORS


- Chemical Manufacturing and Distribution
- Communications
- Dams
- Emergency Services
- Financial Services
- Government Facilities
- Information Technology
- Transportation Infrastructure
- Commercial Facilities
- Critical Manufacturing
- Defense
- Energy
- Food and Agriculture
- Healthcare
- Nuclear Reactors
- Water/Wastewater













60% Of Organizations Would  
Consider Paying In The Event  
Of A Ransomware Attack,  
With 1 In 5 Potentially Willing  
To Spend 20% Or More Of  
Their Annual Revenue




# There is a decent chance I will lose it today.....

- Were you aware that many countries (including our own) do not have specific laws or enforcement policies concerning cyber crimes?
- Or (get this) - Most local infrastructure has no protection. None .. Like, NONE.
- Oh - and there is plenty of proof that there is no correlation between budget and security when it comes to cybercrime.



The reason so many organizations suffer breaches is simply a failure in doing the very basics of security. It doesn't matter how much security technology you buy; *you will fail.*







Do you know why money doesn't matter?

BECAUSE PEOPLE ARE STUPID





## CYBERSECURITY STATISTICS

90%

OF ALL CYBER SECURITY BREACHES OCCUR BECAUSE SOME TYPE OF HUMAN ERROR.

60%

OF ALL ATTACKS WERE CARRIED OUT BY INSIDERS.

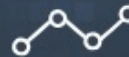
72%

OF PROFESSIONALS ADMITTED THEY WOULD BE WILLING TO SHARE SENSITIVE OR REGULATED INFORMATION IF PROMPTED.



### RANSOMWARE

4,000 RANSOMWARE ATTACKS OCCUR EVERYDAY.



### TARGET AUDIENCE

43% OF CYBER ATTACKS ARE AIMED AT SMALL BUSINESSES.



95% OF BREACHED RECORDS CAME FROM 3 INDUSTRIES- GOVERNMENT, RETAIL & TECHNOLOGY.



91% OF CYBERATTACKS BEGIN WITH SPEAR PHISHING E-MAILS.



We think about  
this entirely the  
wrong way

You must stop thinking of your country,  
your company or your life as a VAULT, and  
more like a fortress.


Vaults are closed and you do everything  
you can to keep people out.

A Fortress you just assume people will  
eventually get in.





# This all starts with strategy

- For a strategy to be sound, it should be preceded by a warts-and-all look at the effectiveness and maturity of the as-is position and a clear line of sight of where it needs to get to. This requires a deep understanding of the business within which security operates, alongside measuring the effects of the myriad security jigsaw pieces across the organization.
  - This almost never happens. If it did, security teams would recognize that investment needs to be made primarily and almost solely on fixing the crap that is already there.
- 

# Policy is pointless.

- We all have policy. Almost every policy is the equivalent of the Ten Commandments: "thou shalt not commit adultery; thou shalt not share thy password."
- The trouble here is that policy is written very much from a position of prejudice by security people for security people. And that isn't smart.
- If your policy is not read or understood, there is little point in having one. Much the same as operating procedures – there is what the policy or procedure says, and then there is the reality of what people do.
- People share passwords ..... Deal with it.



Do you know why policy doesn't matter?

BECAUSE PEOPLE ARE STUPID





# Risk management

---

You know – the continual loop of measurement, planning and action.....REAL risk management.

---

Most organizations deal with theoretical risk (a one-time assessment) and notional controls that “mitigate” the risks found. And then the parameters that make up each risk change, as they have a habit of doing, and nobody notices or reacts because they have no idea how to measure said parameters and act accordingly.

---

Sound familiar? How do you go about measuring each parameter of your security risks? Threat actor/source, threat, exploit, vulnerability/weakness, likelihood, impact, and so on. Do you measure them on an ongoing basis in the context of your organization? Probably not. But you do risk, right?

# There's the rub .....

- Transportation is a critical area of infrastructure outrageously diverse while at the same time, outrageously connected.
- What has created the modern marvel of our logistics infrastructure both creates our problem and our undoing.
- We have networked the stuffing out of this thing.
- And now we are trying to do even more with massive TMS systems.


# Let's just state the obvious shall we?

- Code reviews by authorized independent parties
- Incident response plans that are as connected at the software and companies.
- Drill baby drill.
- Multi-factor authentication: Use it any time it is offered. If it is not offered, consider switching to a software or service that does offer it.

# The simple fix for now


- Passphrases: change passwords to 15-character passphrases.
- It has been reported that some employees at SolarWinds were using "solarwinds123" as their password.
- Any 8-character password can be hacked with modern software in under 3 minutes, but a 13-character password takes 5.2 million years.







"It's a complicated question and topic, and there are lots of different equities that need to be taken into account," Andy Ellis, former CSO at Akamai Technologies

"I see people calling for punishments on people who pay a ransom, which I think is a disaster of an approach. I would much prefer to punish people who take ransom."






•The National Cybersecurity Preparedness Consortium Act of 2021 (S.658), introduced by Senator John Cornyn (R-TX), the bill allows the **DHS** to work together with a consortium of nonprofit entities to develop, update, and deliver cybersecurity training in support of homeland security.





# Vessels, Ships and Ports

- Testing, analysis and planning for ports, airports and vessels needs to be a legal requirement.
  - This ought to be driven by insurance companies and paid for by the carriers and owners.
  - Believe it or not, this may a problem solved by autonomous vehicles.
- 


# Trucks – probably our first problem

- Less than half (43%) of trucking and logistics organizations have a chief information officer (CIO).
- These findings underscore two problems. First, not having a CISO means a company probably doesn't have a formal plan in place for addressing threats either. Second, in the view that they don't need a CISO, most entities implicitly ignore the importance of a good defense. If you don't believe you need expert guidance in the first place, you won't get an expert to deal with it.





# Honor Amongst Thieves

- This ridiculous notion that there are “off limits” industry or sectors of the economy is a fantasy that only politicians can embrace.
  - It’s kind of like the mafia agreeing only to involve themselves in certain kinds of crime.
  - Spare me.
- 

# Get Aggressive

- Do we really need to have this much visibility to everything?
- TAPA Cyber Standard
- A “Proactive Approach” by crypto currency and the “industry” around it.
- Go on the offensive – NOW. Not just this country, but you as a company.

# No More Mr. Nice Guy


- The US Has held countries responsible for the actions of criminals before. Time to kick it up a notch.
- Incentivize firms to harden their defenses through dollar-for-dollar tax credits.
- Give a little to get a lot, create an international coalition to deal with the hackers and give in on Russian sanctions in exchange for cooperation.

# No More Mr. Nice Guy

- Private counter cyber teams (commando nerds!)
- Some people are even going so far as to consider making cyber insurance illegal, but that won't be a problem soon. It will be so expensive that nobody will be able to afford it or qualify for it.
- Premiums are already up 27% over last year on average.



# The Government Isn't Going to Fix This

- The government just can't, and you don't want them doing it either.
  - The role they play is to prosecute the bad guys once something has gone wrong, not to protect you.
  - YOU NEED TO PROTECT YOU.
- 





# Prometheus

---


Prometheus has adopted a very professional approach to dealing with its victims – including referring to them as "customers,"

---

Members of the group communicate with victims via a customer service ticketing system that includes warnings on approaching payment deadlines and notifications of plans to sell stolen data via auction if the deadline is not met.

---

Prometheus appears to be selling stolen databases, emails, invoices, and documents that include personally identifiable information.



# Figure it Out Folks

Pete Mento

President

Mento LLC

AND ...

Partner

UNDENIABLE TECHNOLOGIES

978.317.3250

Pete.Mento@MentoLLC.com

