Digital Safety

"Keeping Humans Safe in a Modern Technological World"

Andy Prow and Barry Green, Co-Founders, Qubit Cyber and Nigel Hanson, Digital Safety NZ

Andy:

- *Software Dev – Pen Tester*
- *Founder of Aura InfoSec*
- *Founder of RedShield*
- *Co-Founder of Qubit Cyber*
- *Board Member for NZTech*
- *NZTech's Digital Safety Board Chair*
- *PhD Student*

Barry:

- *Head of Security, Akamai*
- *Global Security Lead, Cisco*
- *Global Security Lead, Juniper*
- *Global Tech-Lead, ShadowServer*
- *Global CERT and IR Responder*

Cyber Security:

*"is the application of technologies, processes, and controls to protect **systems**, **networks**, **programs**, **devices** and **data** from cyber attacks." (gov.uk)*

*"is the art of protecting **networks**, **devices**, and **data** from unauthorized access or criminal use" (US CERT)*

*"is the protection of **computer systems** and **networks** from information disclosure, theft of, or damage to their hardware, software, or electronic data" (Wikipedia)*

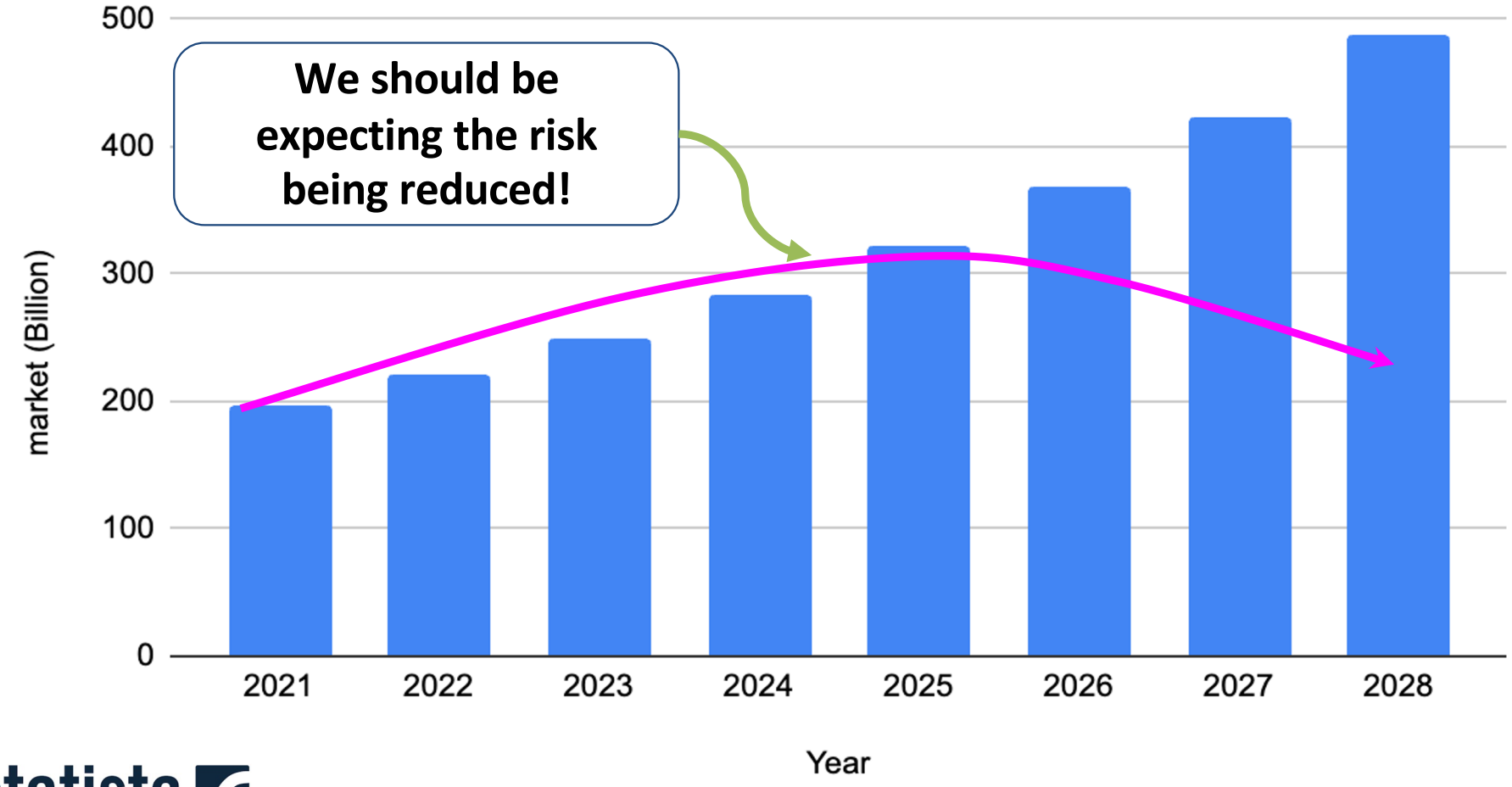
Digital Safety:

“Safety of your data, and your finances”
(Data breaches, PII, PHI, scams)

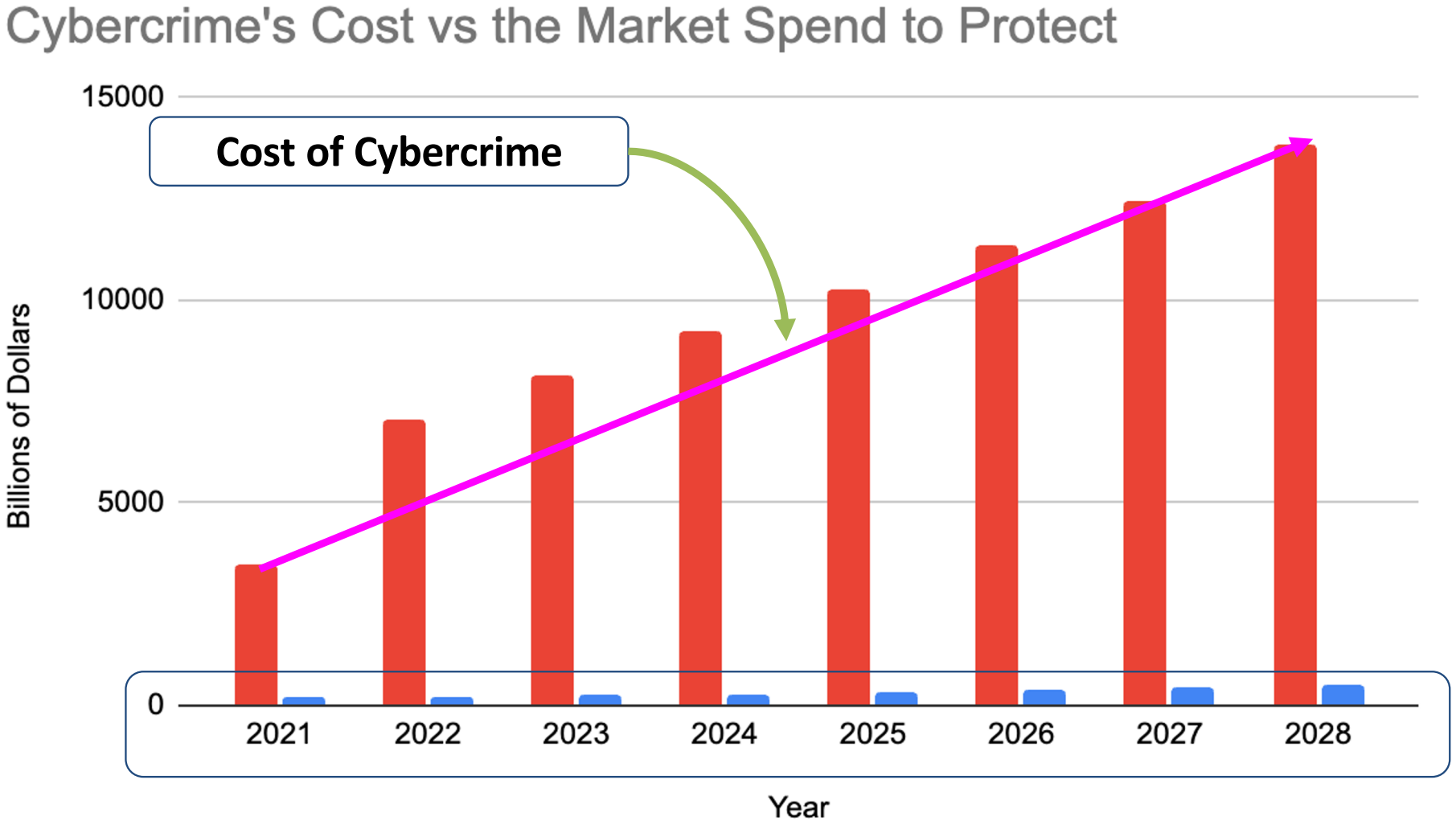
“Harm to your digital self or online persona”
(Online bullying, sextortion, stress / mental harm / physical harm…)

“Real-world health and safety”
(Planes, trains, automobiles, med-tech, agri-tech, drone-tech, CNI, manufacturing, IoT, smart-everything, AI…)

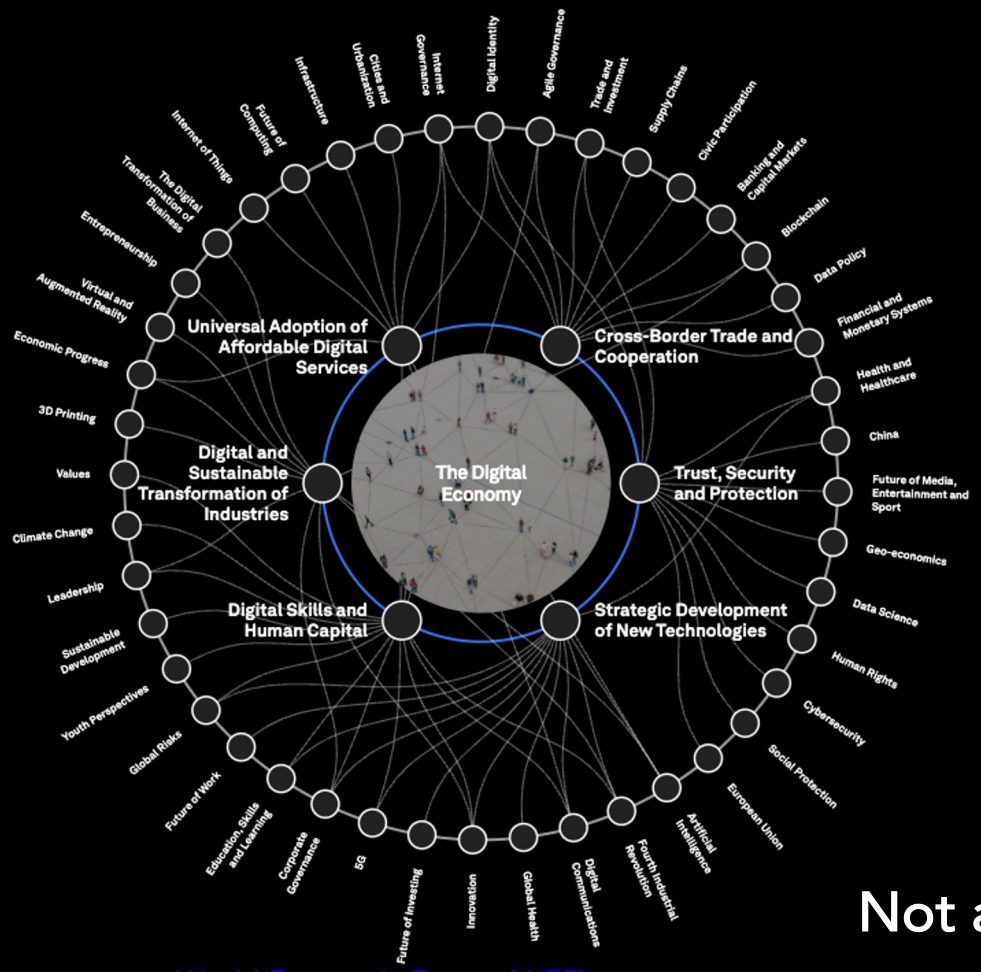
Cybersecurity Market Opportunity



statista


Cybercrime's Cost vs the Market Spend to Protect
Cost of Cybercrime
15000
10000
5000
0
Billions of Dollars
2021
2022
2023
2024
2025
2026
2027
2028
Year

Where cybersecurity is heading today .....



World Economic Forum (WEF)

.... protecting .....

.... assets .....

.... economies ....

.... business data ....

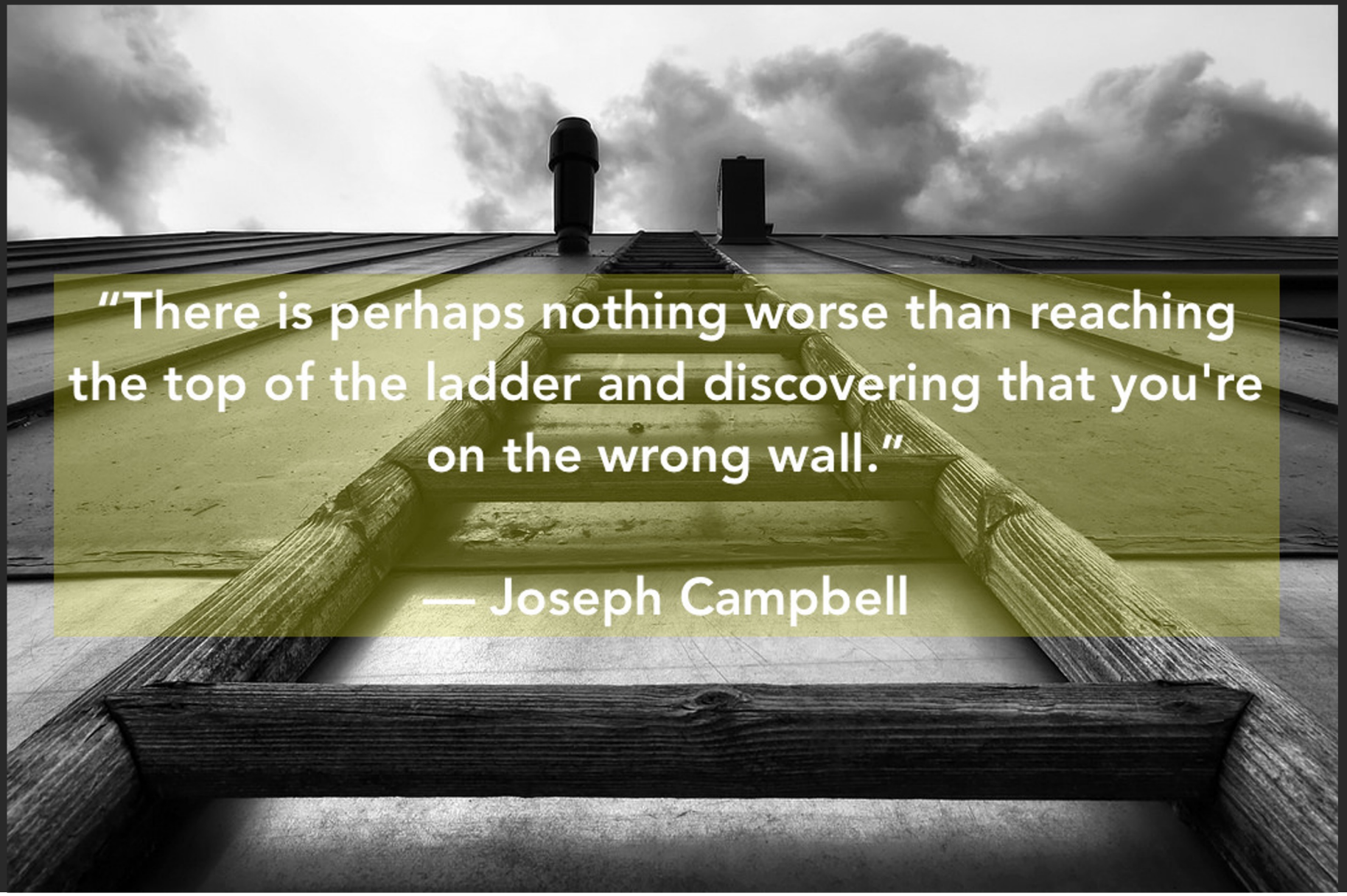
.... Global Trade ....

.... standards to enable more ....

.... "transactional" trust ....

.... Skilled Cyber Workers ....

Not about real-world people's safety!


"There is perhaps nothing worse than reaching the top of the ladder and discovering that you're on the wrong wall."
— Joseph Campbell

Cyber-kinetic attack

From Wikipedia, the free encyclopedia

A **cyber-kinetic attack** targets cyber-physical systems and causes direct or indirect physical damage, injury or death, or environmental impact solely through the exploitation of vulnerable information systems and processes.[1] Notable attacks in this category in the recent past have targeted critical infrastructure facilities such as water treatment plants,[2] nuclear power plants,[3] oil refineries,[4] and medical facilities.[5]

Crossing the cyber-physical divide [edit]

Colonial Pipeline - cyber-criminal attacks intensify

In May 2021, a state of emergency was declared in a number of US states after hackers **caused a vital oil pipeline to shut down**.

Fears over fuel shortages spurred some US consumers to panic buy petrol

Colonial Pipeline carries 45% of the east coast's supply of diesel, petrol and jet fuel and the supply led to panic at the pumps.

This attack wasn't carried out by Russian government hackers, but by the DarkSide ransomware group, which is thought to be based in Russia.

The pipeline company admitted to paying criminals $4.4m in hard-to-trace Bitcoin, in order to get computer systems back up and running.

Recovering from the global tech outage could be a long, arduous process

By Brian Fung, CNN

7 minute read · Updated 2:25 PM EDT, Fri July 19, 2024

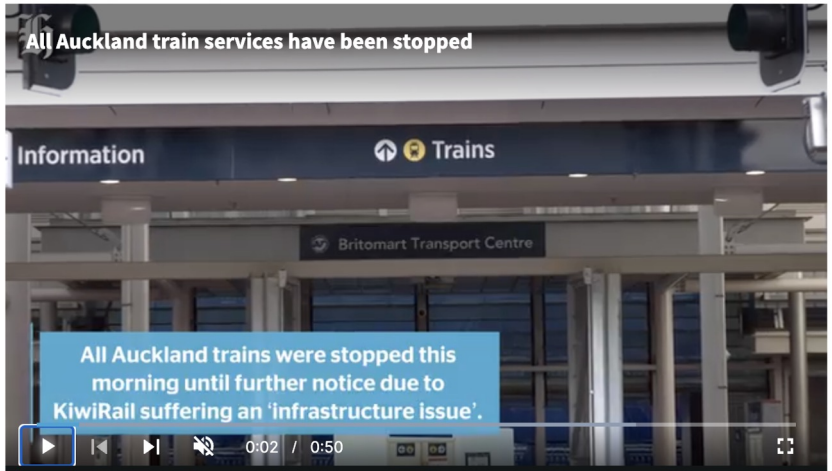
Travelers wait in Terminal 1 for check-in at Hamburg Airport, in Hamburg, Germany, Friday July 19, 2024. A widespread Microsoft outage disrupted flights, banks, media outlets and companies around the world on Friday. Bodo Marks/AP

KiwiRail says Auckland rail network signal failures caused by IT staffer conducting unsanctioned work

By Benjamin Plummer

22 Feb, 2024 08:00 PM · 5 mins to read

Save | Share



KiwiRail has revealed this morning's signal failures across the Auckland rail network were caused by an IT staffer doing unsanctioned work on the rail's firewall.

STONKAM®

HOME ABOUT US AI PRODUCTS SOLUTIONS NEWS CONTACT US EN

HOME > AI> Inside the Vehicle

Inside the Vehicle | Outside the Vehicle

DMS Monitoring

Through multi-layer neural network technology, video image analysis technology, clustering and neural network algorithm, any abnormal driving behaviors (fatigue, distraction, smoking, calling, no mask) during driving can be accurately and real-time monitored, both visual and audio alarms will be actively offered to remind drivers to work properly and drive safely. This algorithm also support driver face detection and authentication, no driver status detection.

View More

Face Recognition Technology

DMS Monitoring

DMS Monitoring

Automatic Passenger Counting

STONKAM®

HOME ABOUT US AI PRODUCTS SOLUTIONS NEWS CONTACT US EN

HOME > AI> Outside the Vehicle

Inside the Vehicle | Outside the Vehicle

Pedestrian Detection (PD) Technology

Pedestrian detection technology, which is a deep learning technology based on big data, can intelligently detect whether there are targets such as pedestrians and cyclists in front of the vehicle, meanwhile it could accurately analyze information such as the speed and distance between the vehicle and the target object. When a risk of collision is predicted, an alert will be triggered to avoid a collision.

View More ›

Forward Collision Warning (FCW)

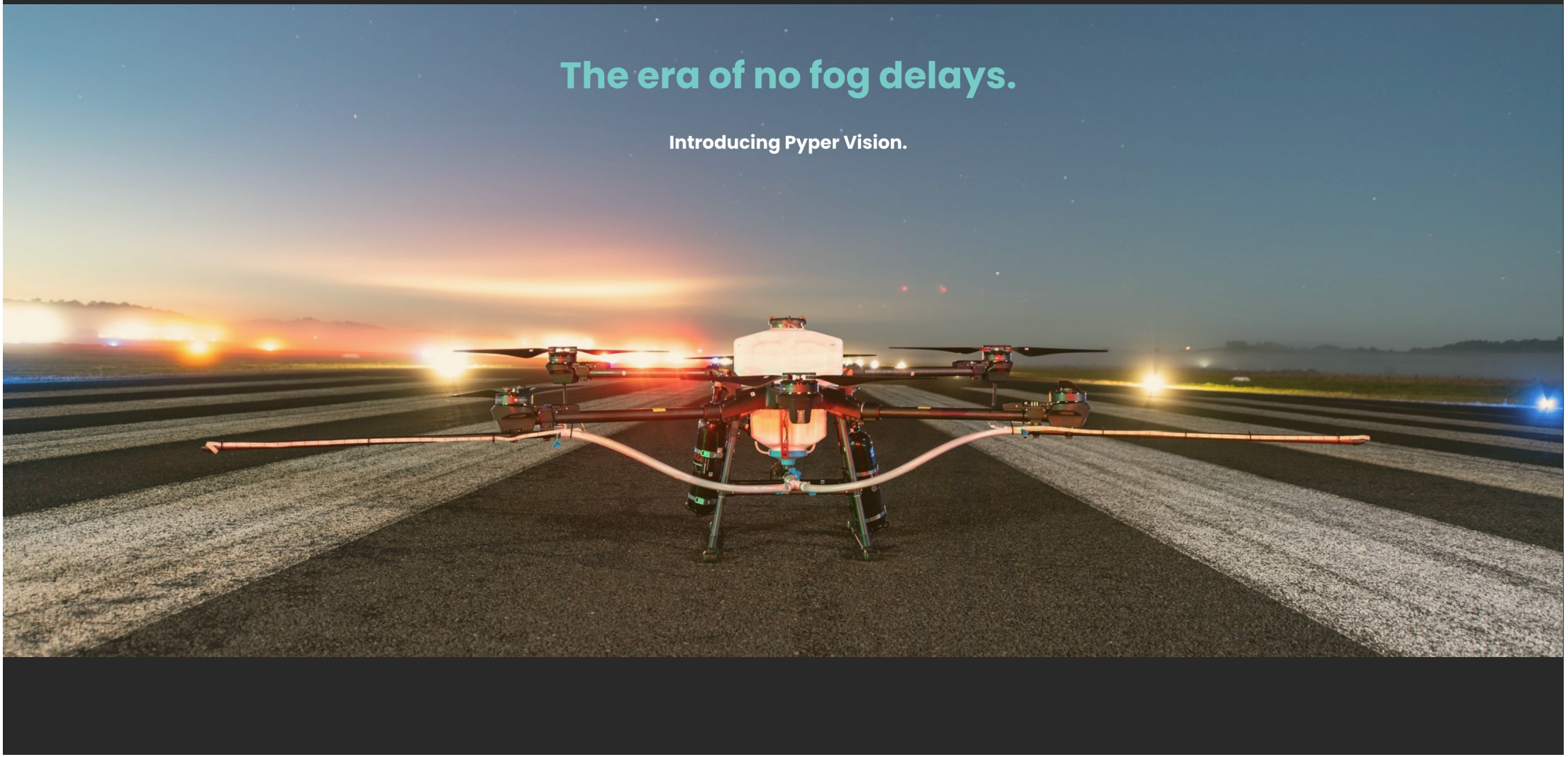
Lane Departure Warning (LDW)

The Preceding Car Starting Reminder

Pedestrian Detection (PD)

Pedestrian Detection (PD)

Speed Sign Recognition (SSR) & Over speed Alarm


The era of no fog delays.
Introducing Pyper Vision.

WIRED

SUBSCRIBE

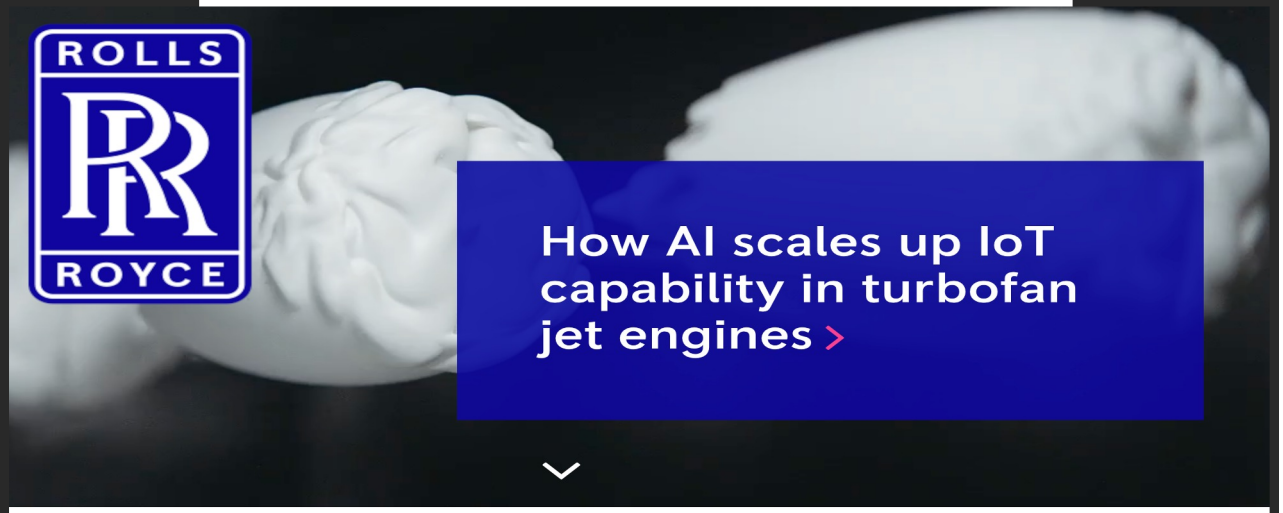
ASHLEY BELANGER, ARS TECHNICA

BUSINESS FEB 17, 2024 12:12 PM

Air Canada Has to Honor a Refund Policy Its Chatbot Made Up

The airline tried to argue that it shouldn't be liable for anything its chatbot says.

According to Air Canada, Moffatt never should have trusted the chatbot and the airline should not be liable for the chatbot's misleading information because, Air Canada essentially argued, "the chatbot is a separate legal entity that is responsible for its own actions," a court order said.



In a realisation of its IntelligentEngine vision, Rolls-Royce has pioneered a new technical solution – using AI and IoT together to build smarter jet engines.

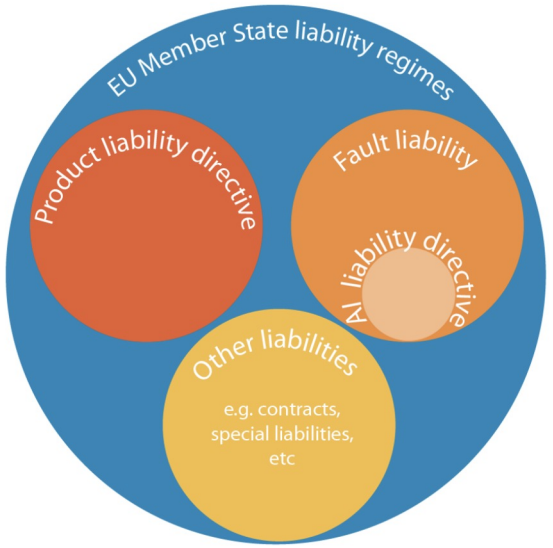
Who's Liable?

The AI liability directive concerns 'extra-contractual' civil liability rules, i.e. rules providing a compensation claim irrespective of a contractual link between the victim and the liable person.[19]

The rules would ensure that any type of victim (individuals or businesses) can be compensated if they are harmed by the fault or omission of a provider, developer or user of AI resulting in a damage covered by national law (e.g. health, property, privacy, etc.).

The AI liability directive would not affect existing rules laid down in other EU legislation, particularly the EU rules regulating conditions of liability in the field of transport, the proposed revision of the Product Liability Directive or the Digital Services Act. Furthermore, while the AI liability directive does not apply with respect to criminal liability, it may be applicable with respect to state liability given that state authorities are subject of the obligations in the AI act.[20]

Figure 1 – Liability regimes in the EU



Source: European Commission, 2022.

PLD and AI liability directive.

The revised PLD proposal aims to modernise the existing EU no-fault-based (strict) product liability regime and would apply to claims made by private individuals against the manufacturer for damage caused by defective products.

In contrast, the new AI liability directive proposes a targeted reform of national fault-based liability regimes and would apply to claims, made by any natural or legal person against any person, for fault influencing the AI system that caused the damage.

MARCH 27, 2024

Readout: Office of the National Cyber Director Convenes Professors & Think Tank Experts at a Legal Symposium on Software Liability

ONCD Aims to Incentivize Secure Coding Practices to Protect All Software Users

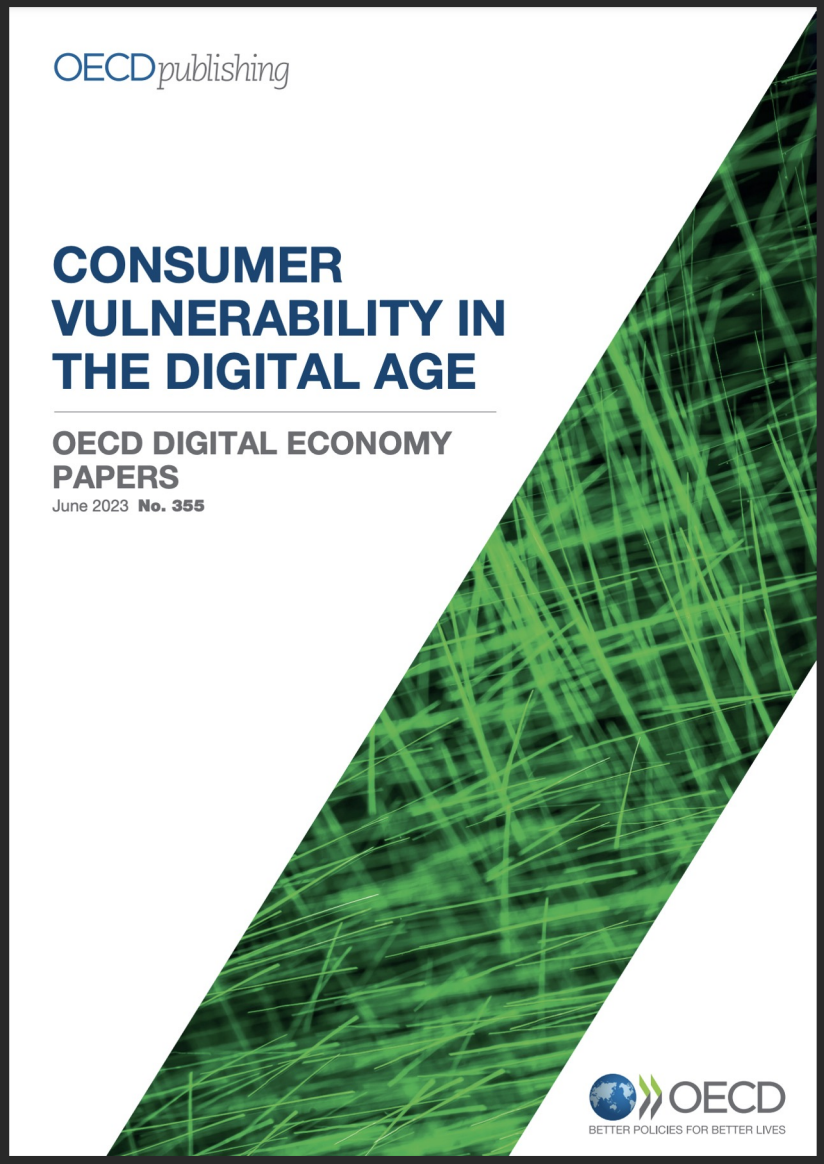
March 27, 2024

OECD

BETTER POLICIES FOR BETTER LIVES

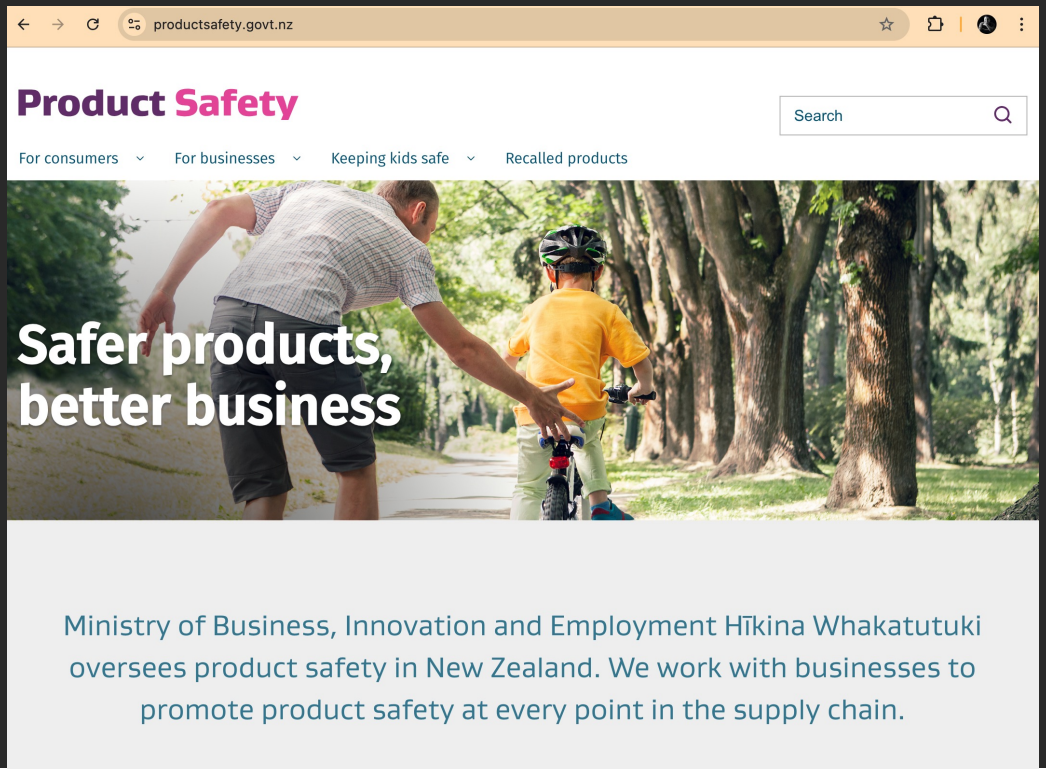
Products incorporating digital technology: What are the risks for consumer safety?

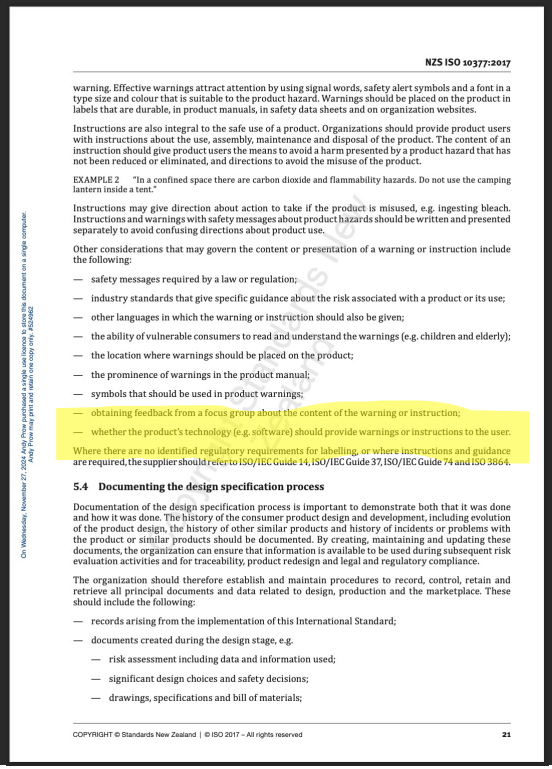
Join us on Thursday, 8 February for a virtual workshop with experts from diverse fields to explore the health and safety impacts of consumer products that use digital technologies like AI, the Internet of Things, and virtual reality.



www.productsafety.govt.nz

- ***"Consider whether the product's technology (e.g. software) should provide warnings or instructions to the user"***





NZS ISO 10377:2017

warning. Effective warnings attract attention by using signal words, safety alert symbols and a font in a type size and colour that is suitable to the product hazard. Warnings should be placed on the product in labels that are durable, in product manuals, in safety data sheets and on organization websites.

Instructions are also integral to the safe use of a product. Organizations should provide product users with instructions about the use, assembly, maintenance and disposal of the product. The content of an instruction should give product users the means to avoid a harm presented by a product hazard that has not been reduced or eliminated, and directions to avoid the misuse of the product.

EXAMPLE 2 "In a confined space there are carbon dioxide and flammability hazards. Do not use the camping lantern inside a tent."

Instructions may give direction about action to take if the product is misused, e.g. ingesting bleach. Instructions and warnings with safety messages about product hazards should be written and presented separately to avoid confusing directions about product use.

Other considerations that may govern the content or presentation of a warning or instruction include the following:

- safety messages required by a law or regulation;
- industry standards that give specific guidance about the risk associated with a product or its use;
- other languages in which the warning or instruction should also be given;
- the ability of vulnerable consumers to read and understand the warnings (e.g. children and elderly);
- the location where warnings should be placed on the product;
- the prominence of warnings in the product manual;
- symbols that should be used in product warnings;
- obtaining feedback from a focus group about the content of the warning or instruction;
- whether the product's technology (e.g. software) should provide warnings or instructions to the user.

Where there are no identified regulatory requirements for labelling, or where instructions and guidance are required, the supplier should refer to ISO/IEC Guide 14, ISO/IEC Guide 37, ISO/IEC Guide 74 and ISO 3864.

5.4 Documenting the design specification process

Documentation of the design specification process is important to demonstrate both that it was done and how it was done. The history of the consumer product design and development, including evolution of the product design, the history of other similar products and history of incidents or problems with the product or similar products should be documented. By creating, maintaining and updating these documents, the organization can ensure that information is available to be used during subsequent risk evaluation activities and for traceability, product redesign and legal and regulatory compliance.

The organization should therefore establish and maintain procedures to record, control, retain and retrieve all principal documents and data related to design, production and the marketplace. These should include the following:

- records arising from the implementation of this International Standard;
- documents created during the design stage, e.g.
  - risk assessment including data and information used;
  - significant design choices and safety decisions;
  - drawings, specifications and bill of materials;

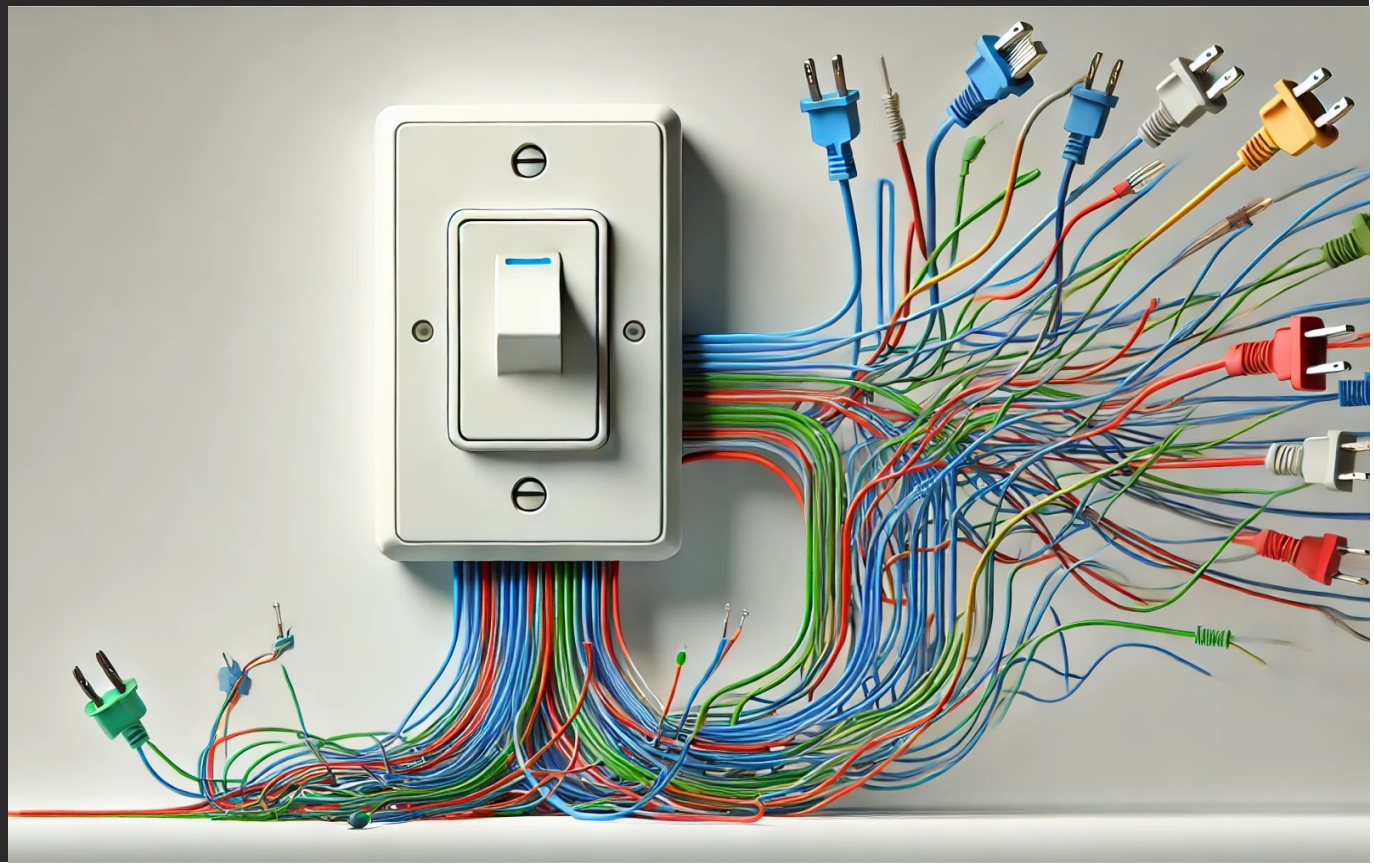

“Digital Safety”
We need to pull the conversation away from
”Is this system secure?”
(Pen-testing, bug-bounties, security patching, vulnerability management, [Dev]SecOps)
to
”Is this product or service safe?”
(Standards, certification, product warranties, liability…)

Principles: Fail Safe and Safely Fail

- ***Risks / Controls***
- ***Safety Measures***
- ***Usage Analysis / Affordance Modelling***
- ***DFMEA (Design Failure Modes and Effects Analysis)***
- ***Consequence Mapping***

Principles: Least Complexity

- *Safety is the inherited from the sum-total of the parts…*
  - *Your code*
  - *3rd party libs (SBOM)*
  - *APIs*
  - *SaaS / PaaS / IaaS*
  - *AI*
  - *SOUP*

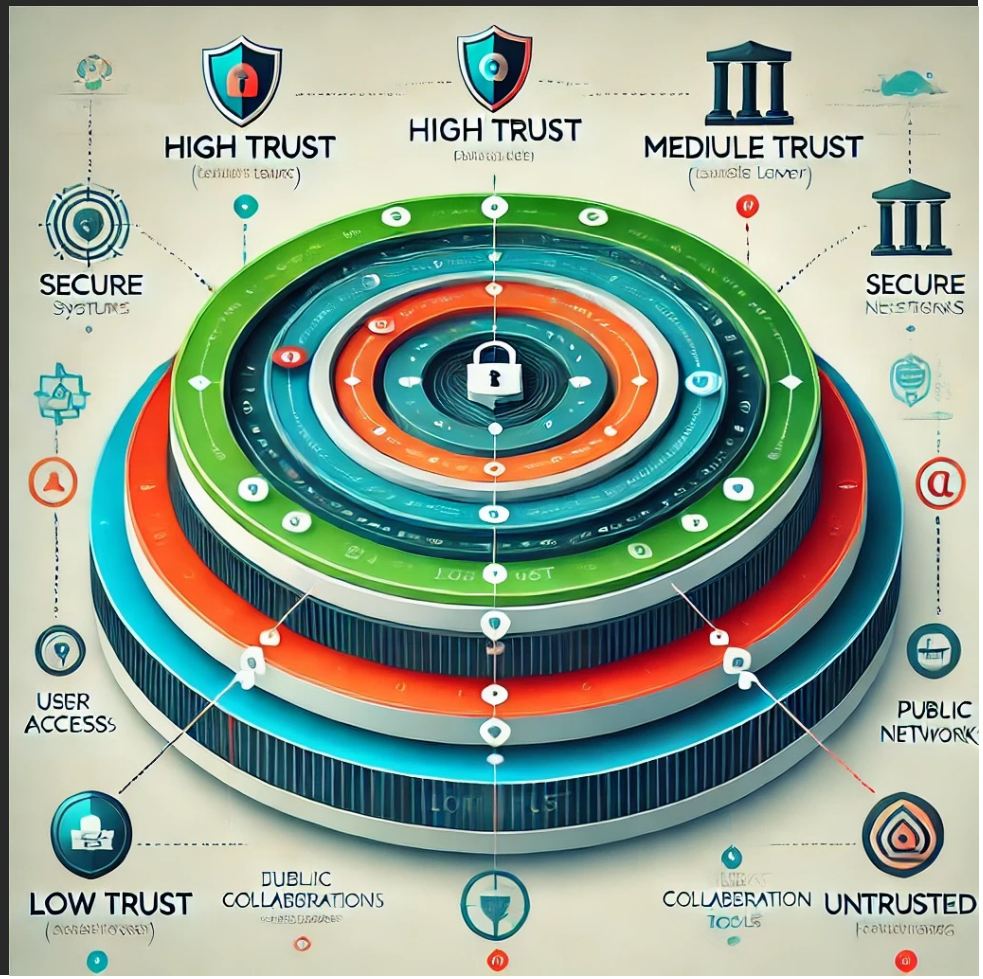


Principles: Model the Physical World

- ***Certified componentry***
- ***Certified professionals***
- ***Professional Indemnity Insurance***
- ***Licensed to operate***
- ***Liability***
- ***Product EOL / Replaceable Parts / Pre-Emptive Maintenance***

Principles: Trust Only When Verified

- ***Flipping the "Trust But Verify"***
- ***Zero-Trust***
  - ***Devices***
  - ***Vendors***
  - ***3rd Party Code***
  - ***Shared Responsibility (for everything)***
- ***"Good brakes make the car go faster…"***



Principles: Democratizing Digital Safety

- ***Let the people choose***
  - ***Transparent***
  - ***Understandable***
  - ***Consistent***
  - ***Mandatory***
- ***DDSR (Device Digital Safety Ratings)***
- ***NOT a TRAINING PROBLEM!***

Pulling It All Together

A City's Transport Tech

Transport Tech Co

A Country's Citizen's Digital Safety

"Democratising Digital Safety"
Building "Digital Trust"

Your Help, Please:

- ***The Good***
  - ***What are you doing that's working? IEC 62443? ISO 26262? NIST CSF? C2M2?***
- ***The Bad***
  - ***What are you doing that's not?***
- ***The Ugly***
  - ***Actual examples of harm?***

Your Help, Please:

- ***FIRST Digital Safety SIG***
  https://www.first.org/global/sigs/digital-safety

- ***Manifesto / The Pledge***

"I will prioritize the safety and well-being of users in all digital systems I work on or influence…"

- ***Digital Safety Roadmaps***
  - ***Country – State – City – Tech Provider***