CHECK POINT

Zero Tolerance Architecture

The Power of Prevention

Antoinette Hodes
Evangelist & Global Solution Architect

The First Cyber Attack…

- Launched in 1834 by two bankers, François and Joseph Blanc
- Manipulated France telegraph data
- Equivalent of an Internet stock fraud

Why Zero Tolerance?

- ✓ Protecting
  - Preventative security controls
- ✓ Ensuring
  - Guaranteed safe and safety
- ✓ Preserving
  - Maintain working as intended

Threat Landscape 2023
IoT and OT

January

Hacktivism

Ghostsec is the first to encrypt Remote Terminal Unit (RTU) using ransomware

March

Cyber Warfare

Sandworm/Caddywiper disrupting power grid Ukraine. Wiper - erasing all data. Causing massive blackout

May

Cyber Warfare

Colonial Pipeline Cyber Attack. Exploiting vulnerable VPN system and shutting down operations

June

Propagation attack & lateral movement

RSOCK proxy bot net. 350K compromised assets. Exploiting know vulnerabilities and weak credentials

October

Backdoors

Wyze Cam vulnerability opening reverse shell and allows takeover. Exploiting authentication.

November

White Hat Research

Experts at Cybernews hijacked 27.044 printers, forcing print jobs 5 step manual how to secure a printer

November

Cyber Warfare

Danish critical infrastructure attack using vulnerablies in Zyxel devices. RCE , buffer overflow and takeover. With Sandworm/Caddywiper

Resilience Security Strategies
Safeguarding IoT ecosystems

- ✓ Protect against cyber attacks
- ✓ Data integrity and privacy
- ✓ Trust and user confidence

Mandating Zero Tolerance
Building Trust in IoT

- ✓ Ease of operation
  - Improved profitability
- ✓ Regulations
  - Improved scalability
- ✓ Business continuity
  - Improved reliability

IoT device manufacturing
Device and market challenges

IoT asset vendor challenges

Factory

- Development
- Programming and Testing
- Source Repos
- Build & Release Management

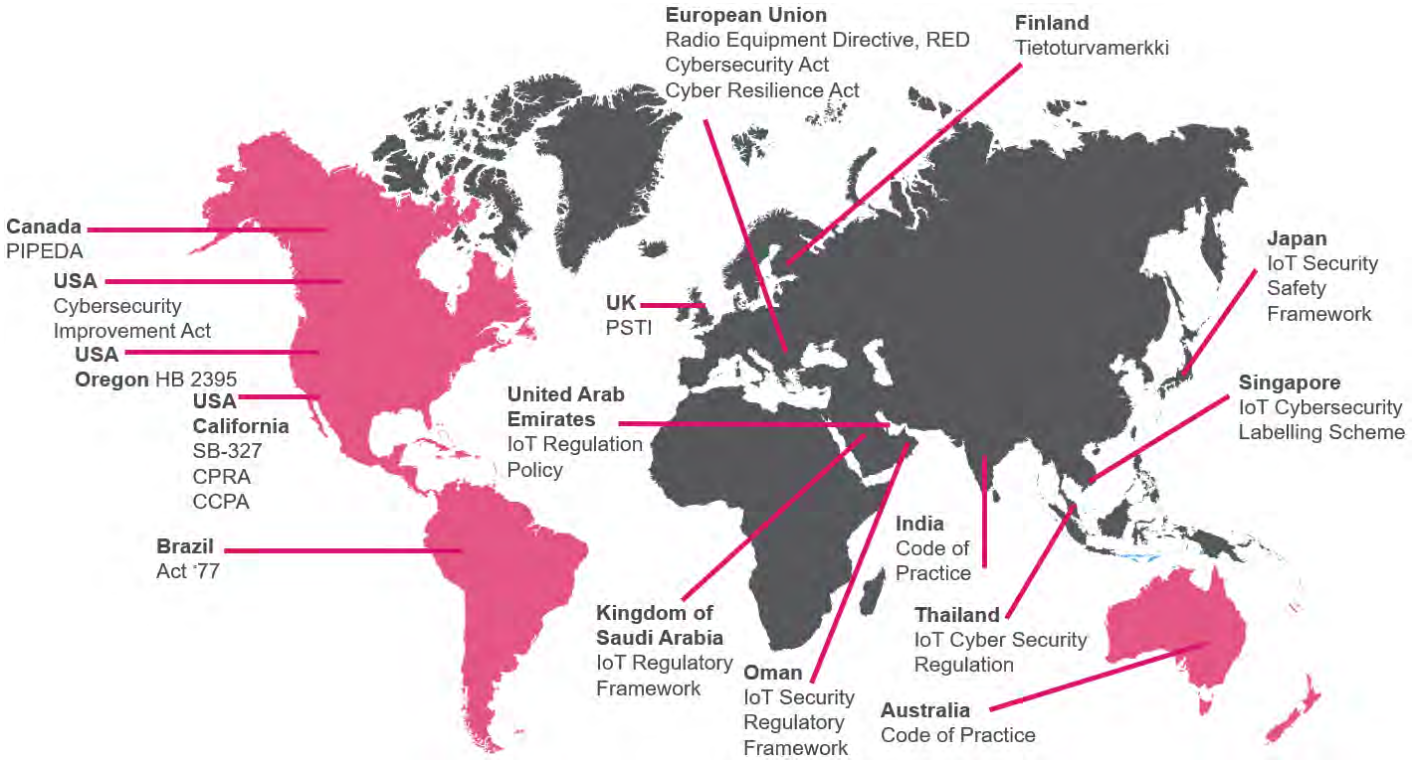
Device Security

- Secure Debug Lock
- Root of Trust
- Secure Key Storage
- Secure Identity

Global Regulations
Safeguarding the IoT revolution

Legislations

- Cyber Security Act (CSA)
- Cyber Resilience Act (CRA)
- Radio Equipment Directive (RED)
- Digital Markets Act (DMA)
- Digital Operational Resilience Act (DORA)
- ETSI EN 303 645 security standard for consumer IoT devices
- Network and Information Security Directive (NIS2)
- US Cyber Trust Mark
- Product Security and Telecommunications Infrastructure Regime (PSTI)



Regulations and standards
Key Elements

- Secure Access and Access Control
- Authentication and Authorization
- Data Protection

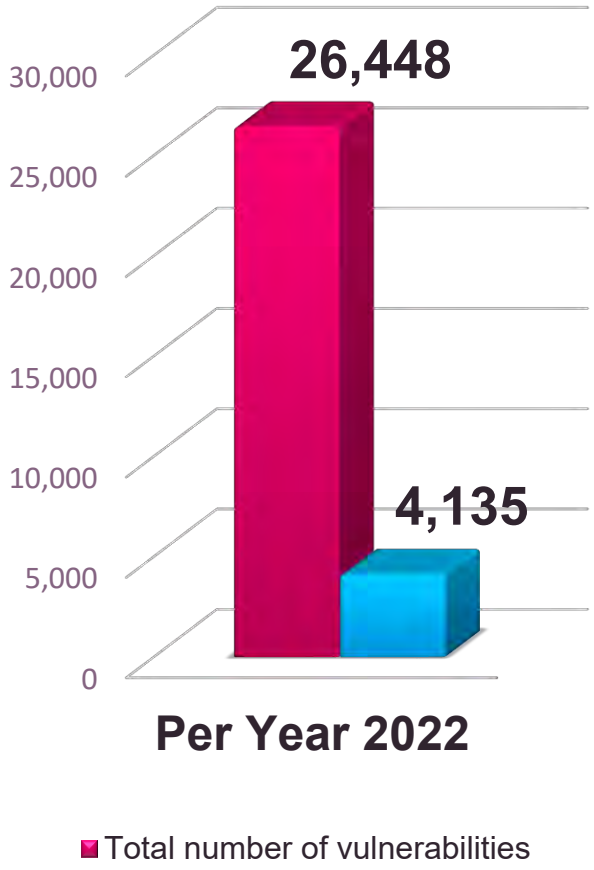
Uncovering Astounding Facts

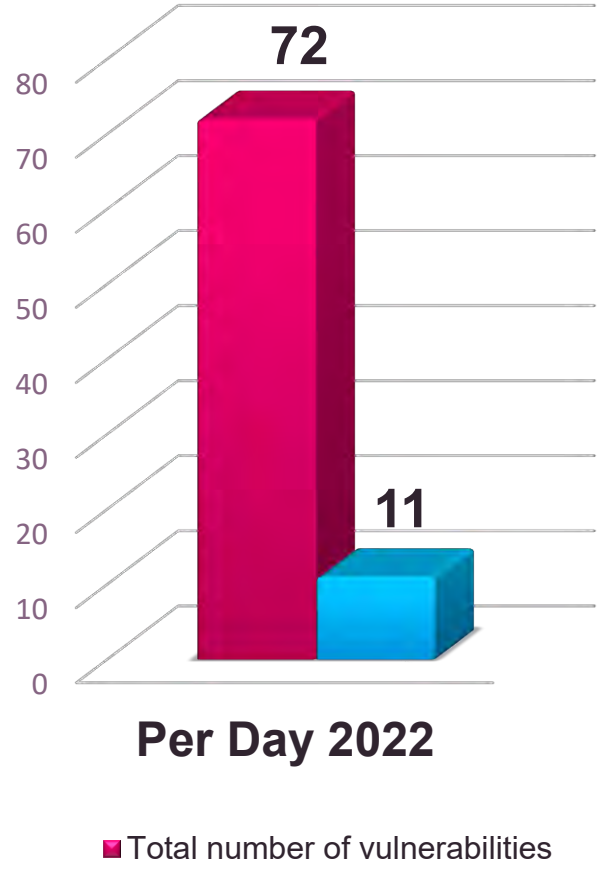
Year 2022

NIST scores security flaws
assigns severity, risk and impact

A critical vulnerability
ranges between 9 and 10

Every day
On average organizations face > 11 critical vulnerabilities



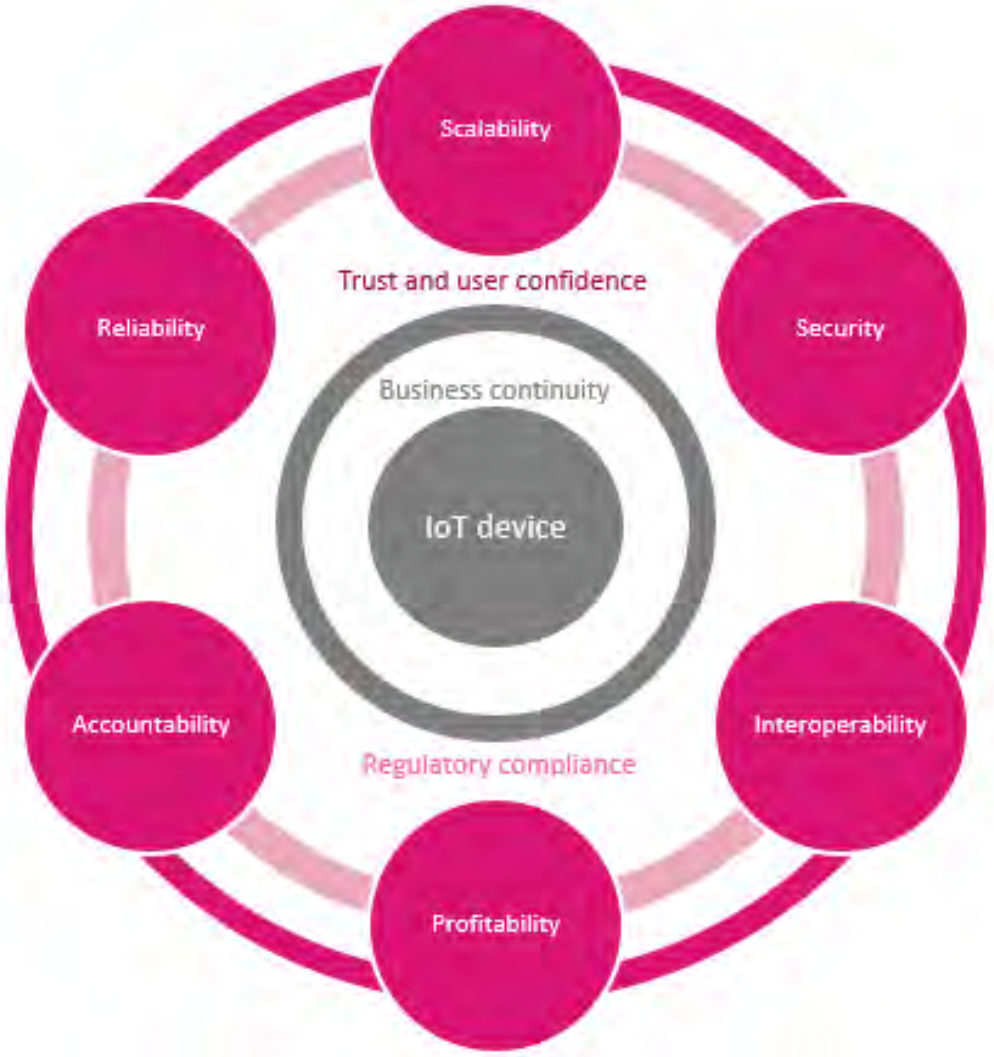


Source: https://www.thestack.technology/analysis-of-cves-in-2022-software-vulnerabilities-cwes-most-dangerous/

Zero Tolerance Architecture

Scalable | Profitable | Reliable

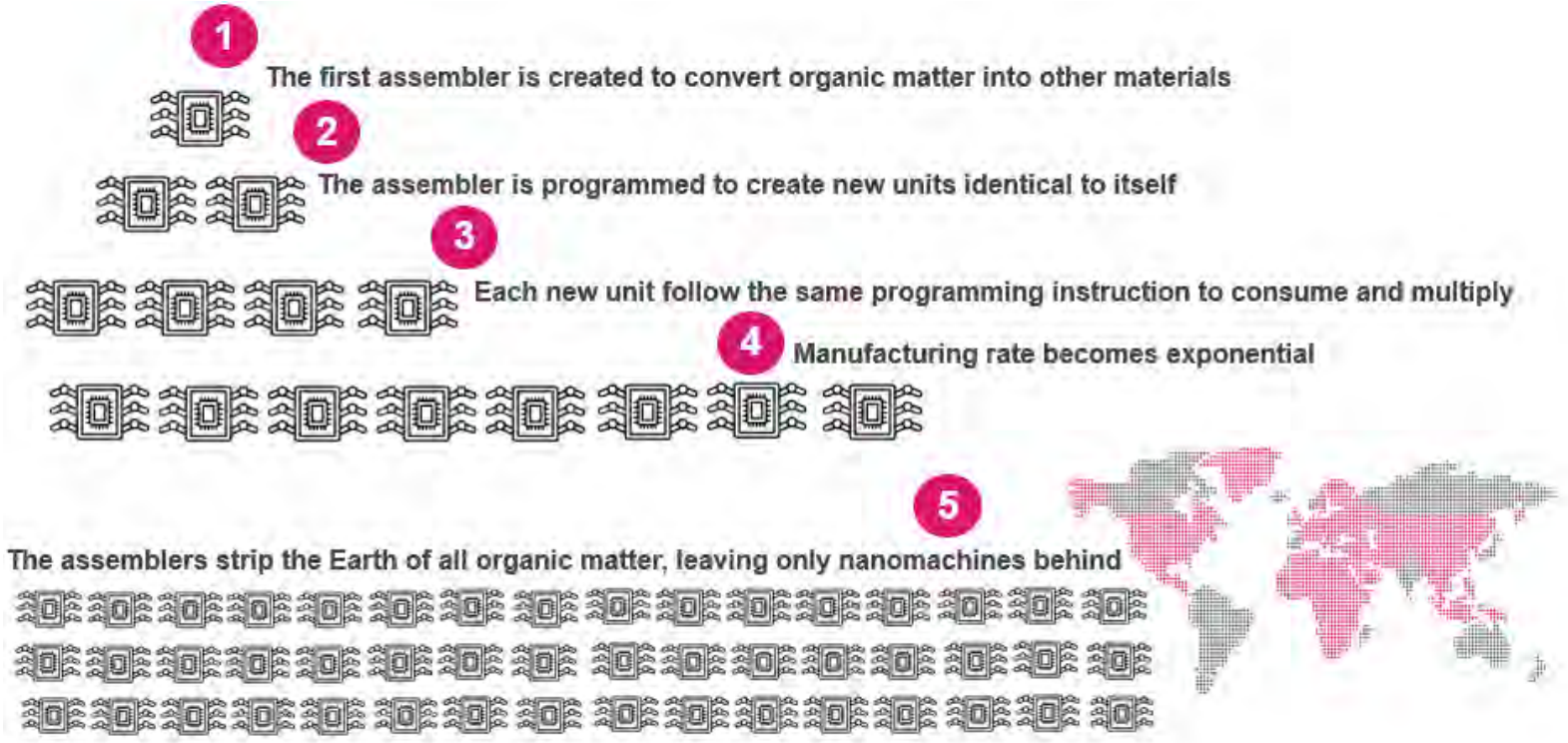
**Save a toaster,
and possibly the world!**



The future of IoT

From algorithms, machine learning to artificial intelligence

1980's - Eric Drexler's "Gray Goo" - book Engines of Creation



https://en.wikipedia.org/wiki/Gray_goo

CHECK POINT™

Robert Mueller, former Director of the FBI

There are only two types of companies:

Those that have been hacked and those that will be hacked

Check Point is adding third one:

Those that have been hacked but still don't know

antoinetteh@checkpoint.com

LinkedIn Antoinette-Hodes @BitWarriorCP

Appreciation bytes -
Thanks for geeking out with us!

YOU DESERVE THE BEST SECURITY