Cybersecurity

OVL Symposium

innovating safety & security

Introduction Boris Zandstra

Study

Business IT & Management Hogeschool Utrecht

DEKRA Certification

Account manager Lighting & Cybersecurity

Cybersecurity services

Training, Guidance, Testing & Certification

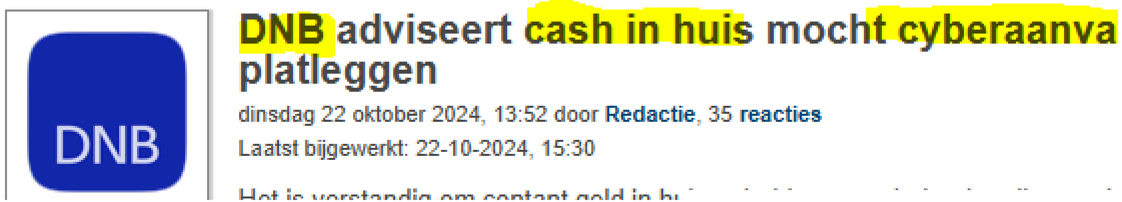
Contact

boris.zandstra@dekra.com

Introduction

- **What is cybersecurity?**
- **The difference in IT & OT**
- **Standards for IT, OT & IoT**

Why is it important to focus on both IT & OT (IoT) for strong cybersecurity?

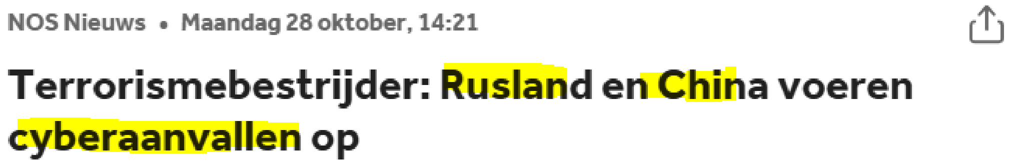


DNB adviseert cash in huis mocht cyberaanva platleggen

dinsdag 22 oktober 2024, 13:52 door Redactie, 35 reacties

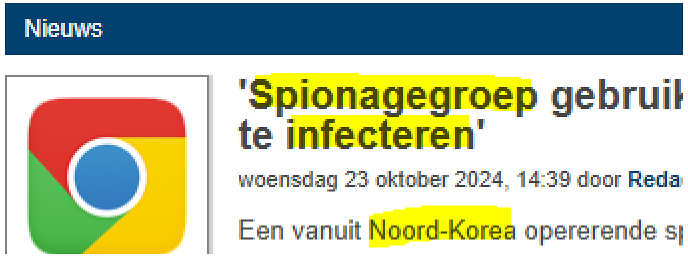
Laatst bijgewerkt: 22-10-2024, 15:30

Het is verstandig om contant geld in hu



NOS Nieuws • Maandag 28 oktober, 14:21

Terrorismebestrijder: Rusland en China voeren cyberaanvallen op

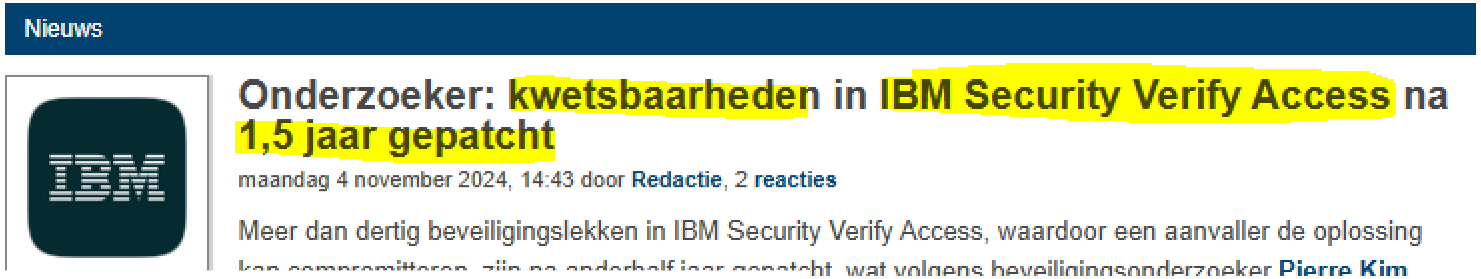


Nieuws

'Spionagegroep gebruik te infecteren'

woensdag 23 oktober 2024, 14:39 door Reda

Een vanuit Noord-Korea opererende sp



Nieuws

Onderzoeker: kwetsbaarheden in IBM Security Verify Access na 1,5 jaar gepatcht

maandag 4 november 2024, 14:43 door Redactie, 2 reacties

Meer dan dertig beveiligingslekken in IBM Security Verify Access, waardoor een aanvaller de oplossing kan compromitteren, zijn na anderhalf jaar gepatcht, wat volgens beveiligingsonderzoeker Pierre Kim

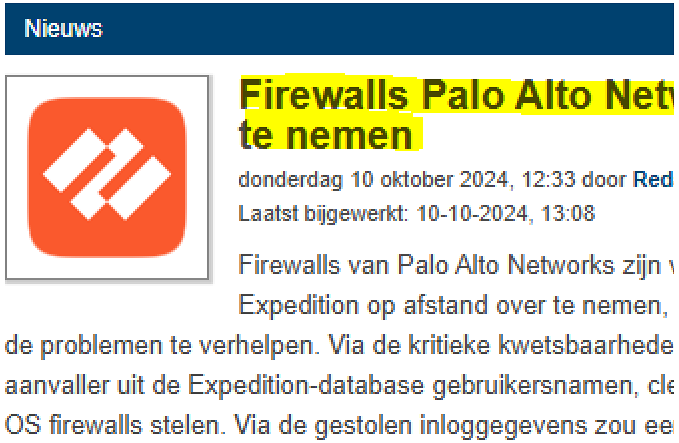
Nieuws

Kamer wil opheldering

woensdag 2 oktober 2024, 14:21 door Redact

Nieuws

GroenLinks-PvdA en D66 willen opheldering over besmette IoT-apparaten



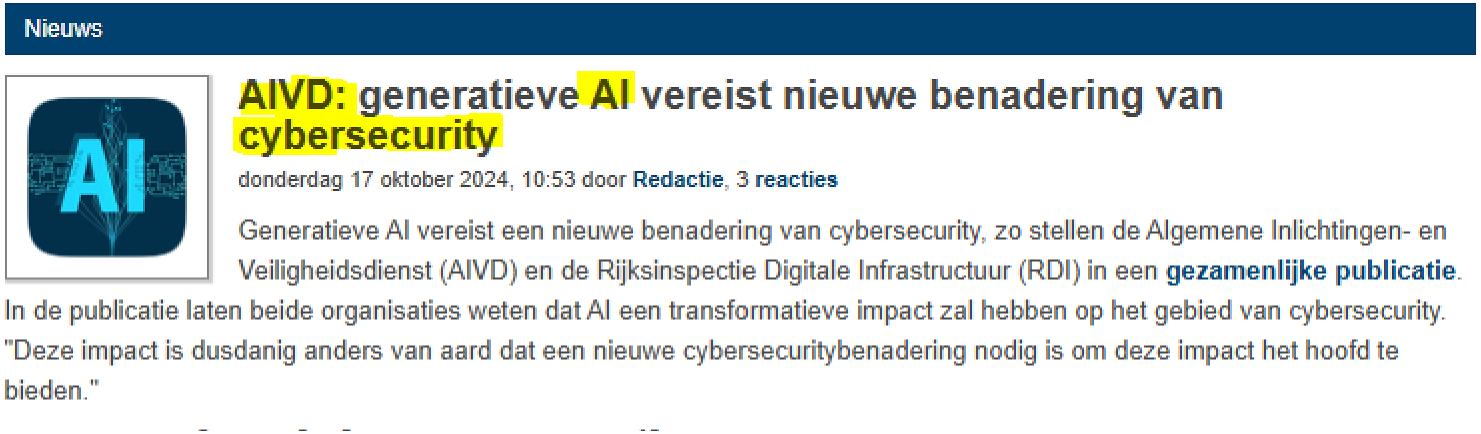
Nieuws

Firewalls Palo Alto Net te nemen

donderdag 10 oktober 2024, 12:33 door Red

Laatst bijgewerkt: 10-10-2024, 13:08

Firewalls van Palo Alto Networks zijn Expedition op afstand over te nemen, de problemen te verhelpen. Via de kritieke kwetsbaarhede aanvaller uit de Expedition-database gebruikersnamen, cle OS firewalls stelen. Via de gestolen inloggegevens zou ee

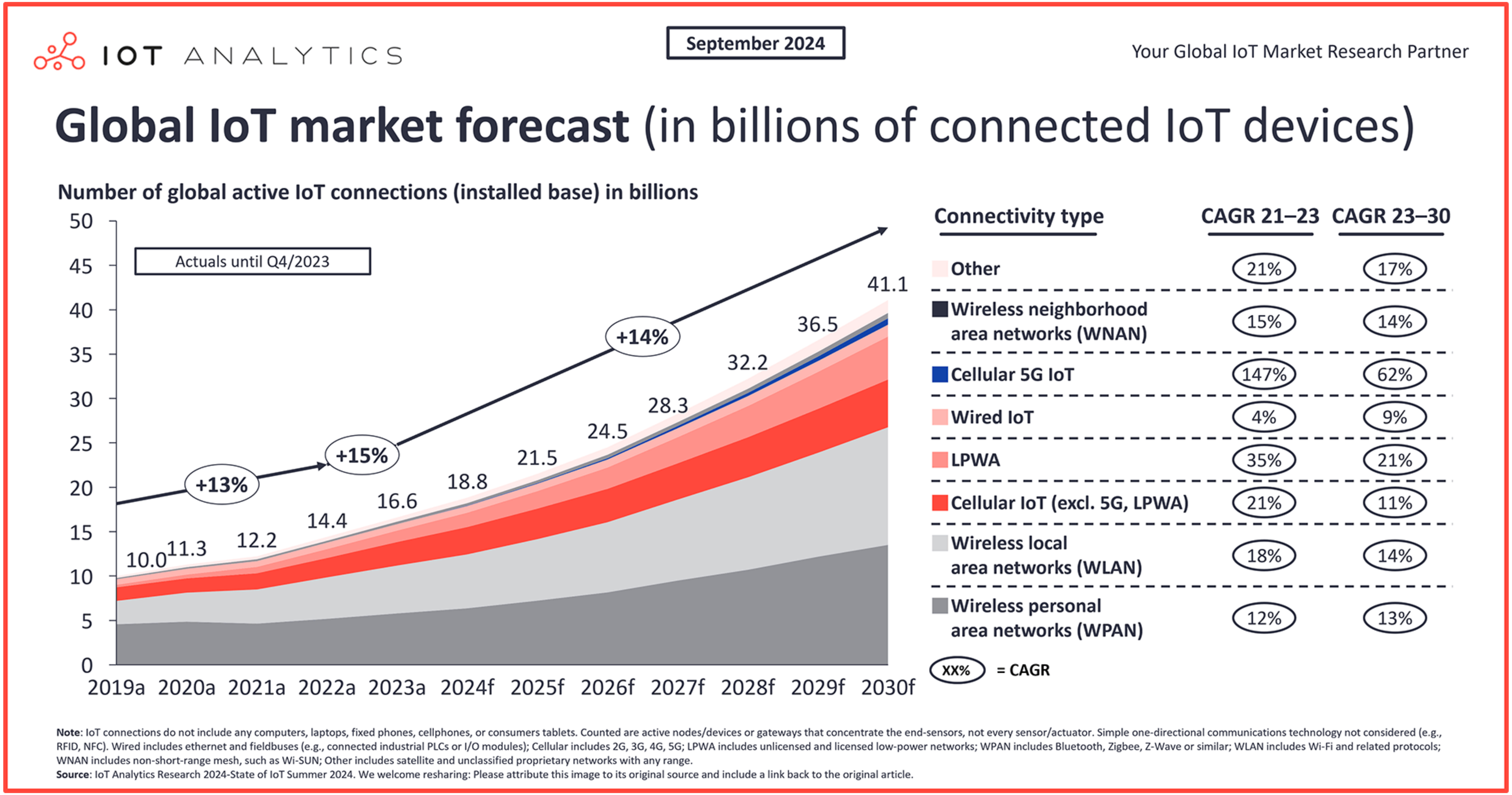


Nieuws

AIVD: generatieve AI vereist nieuwe benadering van cybersecurity

donderdag 17 oktober 2024, 10:53 door Redactie, 3 reacties

Generatieve AI vereist een nieuwe benadering van cybersecurity, zo stellen de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Rijksinspectie Digitale Infrastructuur (RDI) in een gezamenlijke publicatie. In de publicatie laten beide organisaties weten dat AI een transformatieve impact zal hebben op het gebied van cybersecurity. "Deze impact is dusdanig anders van aard dat een nieuwe cybersecuritybenadering nodig is om deze impact het hoofd te bieden."



IOT ANALYTICS

September 2024

Your Global IoT Market Research Partner

Global IoT market forecast (in billions of connected IoT devices)

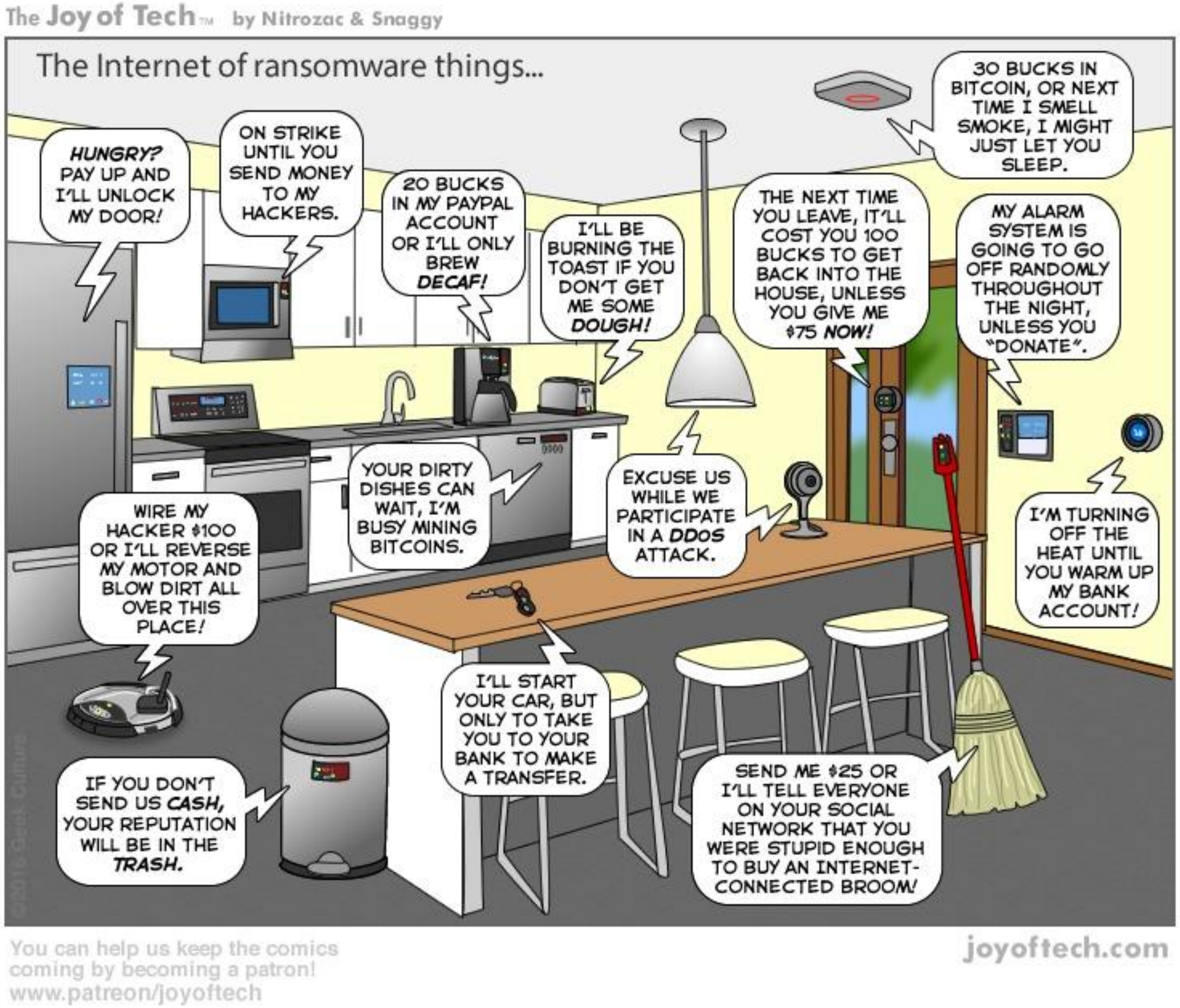
Number of global active IoT connections (installed base) in billions

Connectivity type	CAGR 21–23	CAGR 23–30
□ Other	21%	17%
■ Wireless neighborhood area networks (WNAN)	15%	14%
🟦 Cellular 5G IoT	147%	62%
▨ Wired IoT	4%	9%
▨ LPWA	35%	21%
🟥 Cellular IoT (excl. 5G, LPWA)	21%	11%
▨ Wireless local area networks (WLAN)	18%	14%
■ Wireless personal area networks (WPAN)	12%	13%

XX% = CAGR

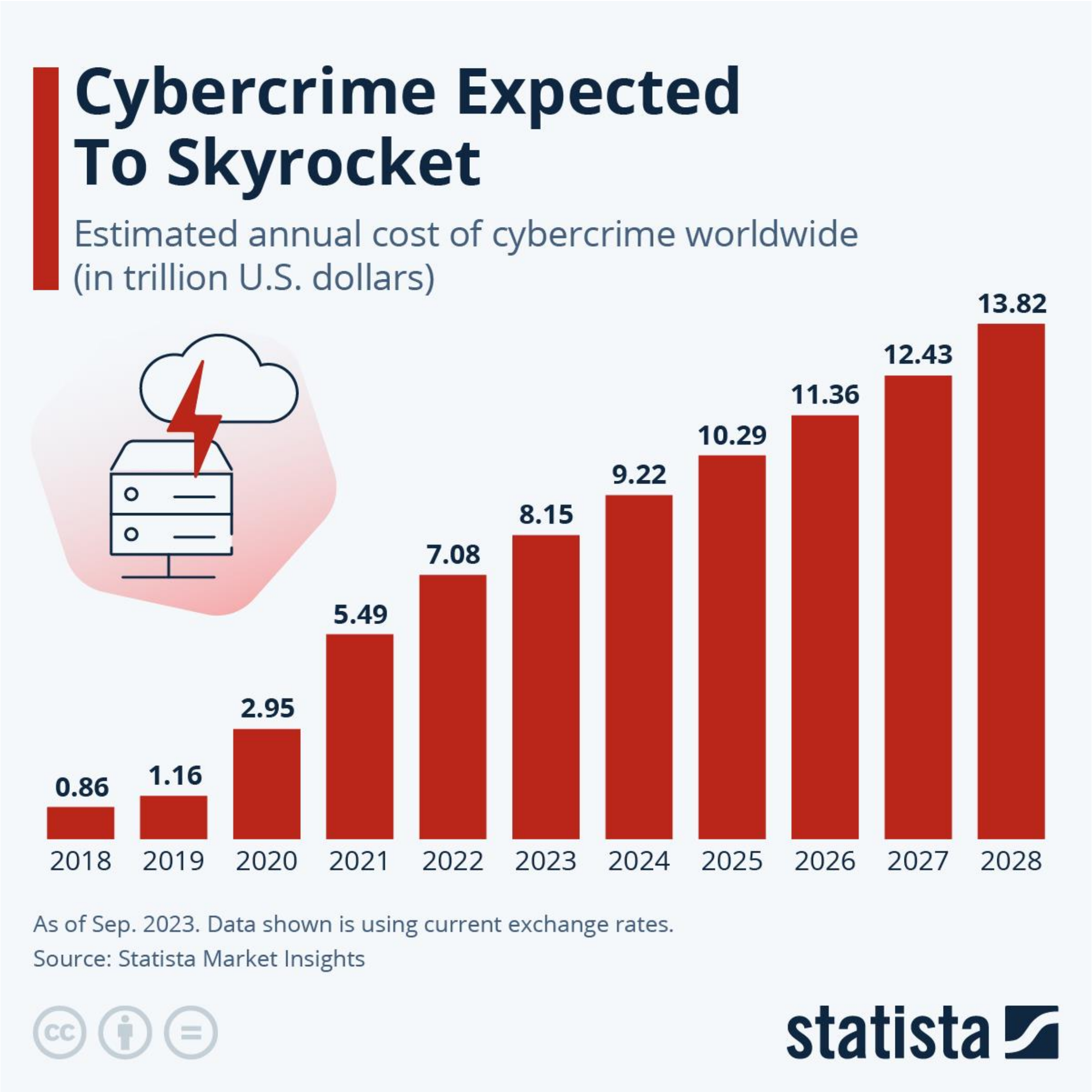
Note: IoT connections do not include any computers, laptops, fixed phones, cellphones, or consumers tablets. Counted are active nodes/devices or gateways that concentrate the end-sensors, not every sensor/actuator. Simple one-directional communications technology not considered (e.g., RFID, NFC). Wired includes ethernet and fieldbuses (e.g., connected industrial PLCs or I/O modules); Cellular includes 2G, 3G, 4G, 5G; LPWA includes unlicensed and licensed low-power networks; WPAN includes Bluetooth, Zigbee, Z-Wave or similar; WLAN includes Wi-Fi and related protocols; WNAN includes non-short-range mesh, such as Wi-SUN; Other includes satellite and unclassified proprietary networks with any range.

Source: IoT Analytics Research 2024-State of IoT Summer 2024. We welcome resharing: Please attribute this image to its original source and include a link back to the original article.


The Joy of Tech™ by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDoS ATTACK.
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
©2016 Geek Culture
You can help us keep the comics coming by becoming a patron! www.patreon/joyoftech
joyoftech.com

Cybercrime is defined:

“damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm.”



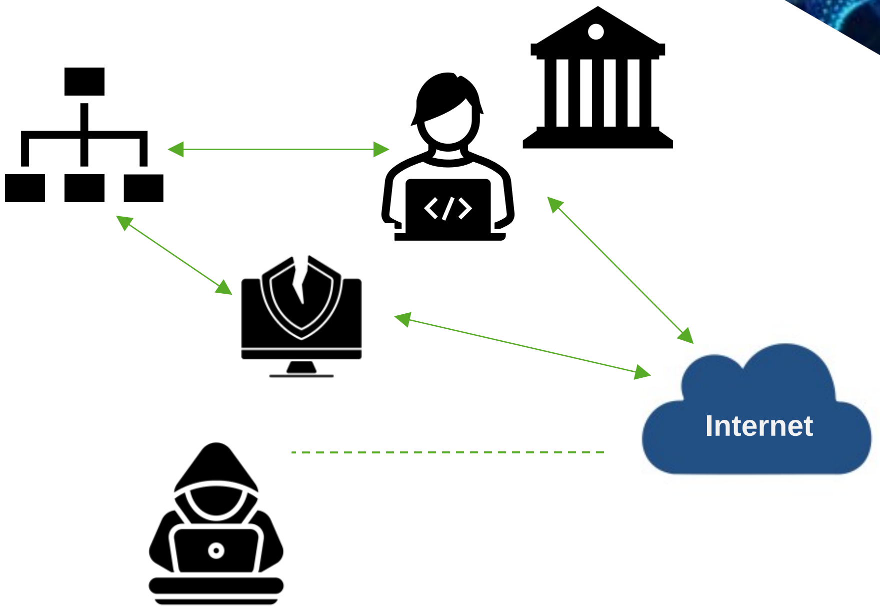
Cybercrime Expected To Skyrocket

Estimated annual cost of cybercrime worldwide (in trillion U.S. dollars)

As of Sep. 2023. Data shown is using current exchange rates.
Source: Statista Market Insights

Weakest link

- Cybercriminals strategically target the most vulnerable points within a system to gain unauthorized access
- Examples:
  - Human errors
  - Outdated software
  - Weak passwords
  - Insider Threats
  - Unsecured networks
  - Unsecured products



Regulation to address cybercrime

The Network and Information Security (NIS-2) Directive

- Affected sectors must create a strategy to procure suitable products for integration into their systems, ensuring no vulnerabilities are introduced

The Radio Equipment Directive

- The RED-Delegated Act introduces cybersecurity requirements for all connected devices with Radio Equipment and is connected needs to comply

The Cyber Resilience Act

- All products with digital elements and services need to comply to strict cybersecurity requirements

Upcoming Regulations

- NIS2 (Q2 2025)
- RED-Delegated Act (1 Agust 2025)
- Cyber Resillence Act (2027)

Regulation to address cybercrime (Standards)

The Network and Information Security (NIS-2) Directive

- ISO 27001 (Essential/critical sectors)
- IEC 62443-2-4 (System integrator)

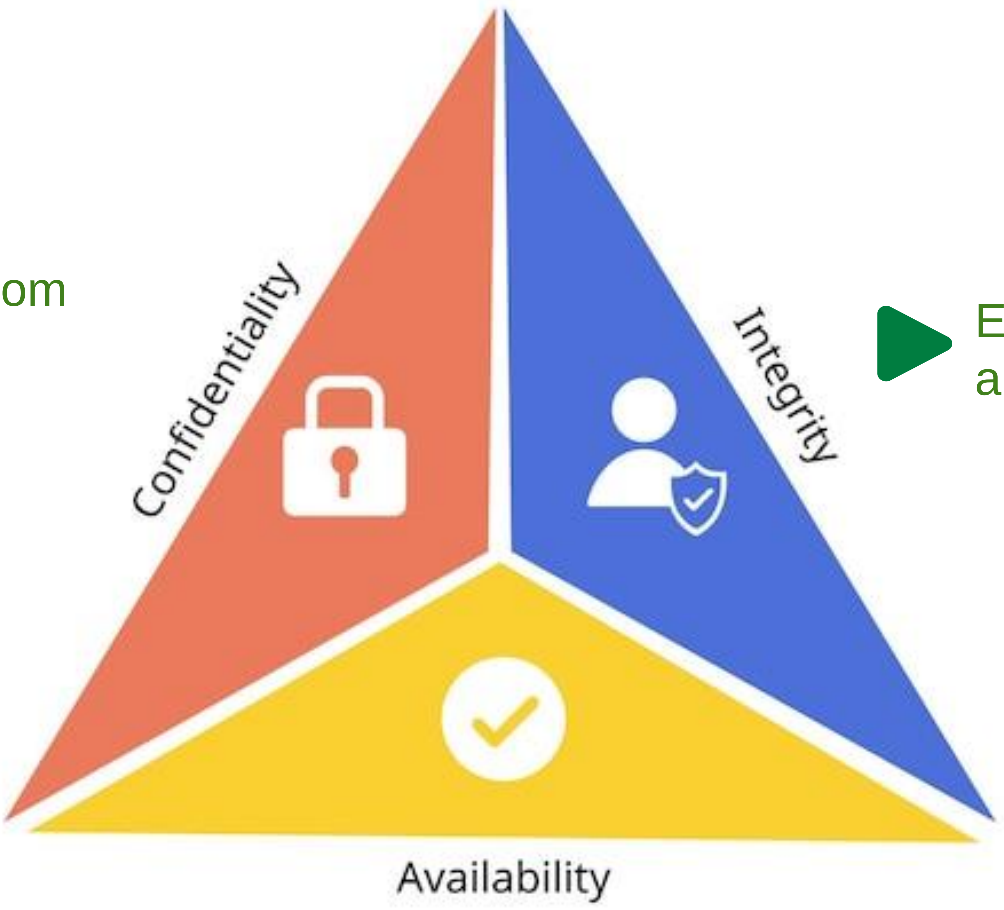
The Radio Equipment Directive

- EN 18031-(1,-2, -3)

The Cyber Resilience Act

- IEC 62443-4-1 & IEC 62443-4-2

CIA Triad



- Keeping information secret from unauthorized people

- Ensure information is accurate and unchanged

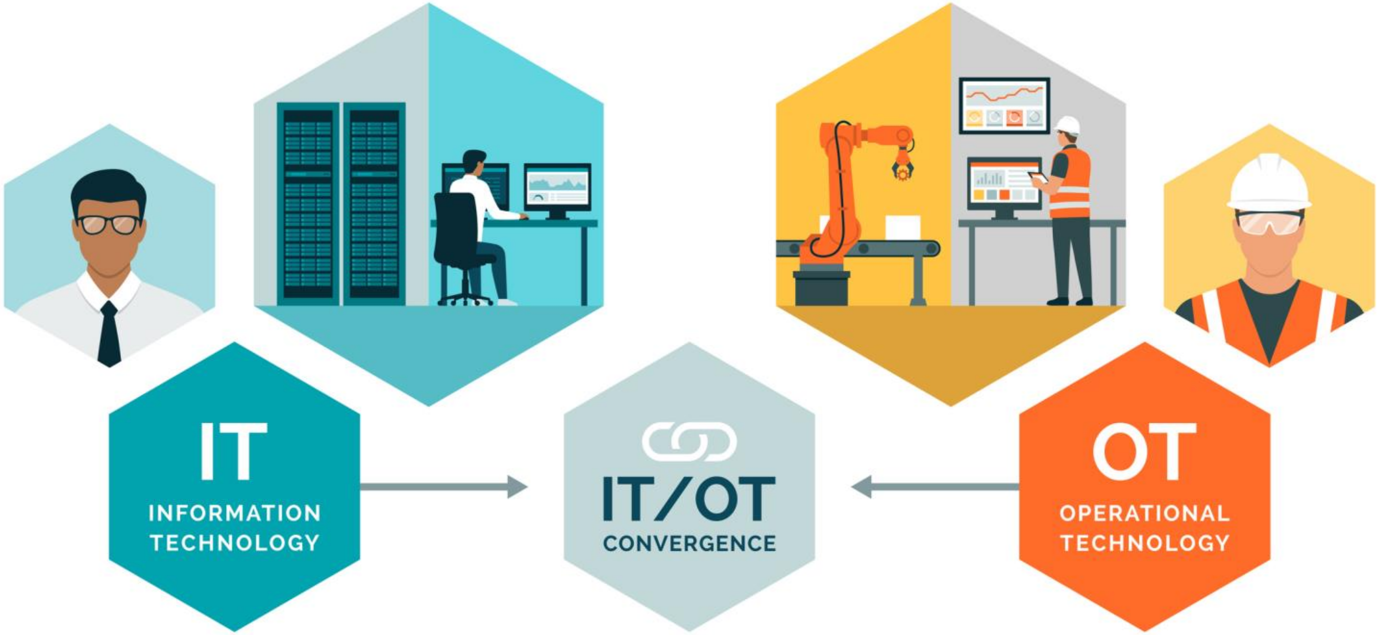
- Making it accessible when needed

IT & OT

Information Technology & Operational Technology

Primary focus: Data management, business operations, and communication

Primary focus: Control and monitoring of physical processes and industrial operations



- ISO 27001

- **Internet of Things**
  - EN 18031
  - ETSI EN 303 645

- IEC 62443

Different focus IT & OT (1)

Information Technology priority

1. Confidentiality
2. Integrity
3. Availability

Confidentiality
Integrity
Availability

Operational Technology priority

1. Availability
2. Integrity
3. Confidentiality

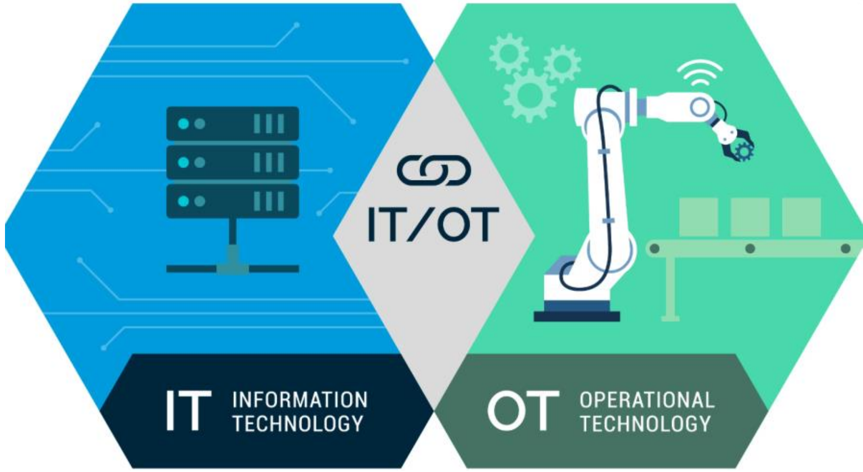
Different focus IT & OT (2)

Key differences

1. **Focus**:
   IT standards focus on protecting data and information systems
   OT standards focus on physical processes

2. **Environment**:
   IT is office based
   OT Industrial/physical

3. **Security measures**:
   IT data encryption, access controls & Incident management
   OT physical controls, Network segmentation & Risk assessments



Different in standard requirements IT & OT

Informatiebeveiliging
ISO/IEC 27001
www.dekra-seal.com
DEKRA
gecertificeerd

ISO 27001

- Access control
- Data Encryption
- Incident management
- Employee training
- ISMS
- Risk Assessment and Treatment
- Regular audits

IEC 62443

- Security program
- Risk Assessment
- Physical Security
- Network Segmentation
- Patch Management
- Control system security
- Operational resilience

Type Approved
Cyber Security
▶ Secure Development Lifecycle
▶ IEC 62443-4-1
▶ Maturity Level 2
www.dekra-seal.com
DEKRA
certified
Cert. ID: xxxxxxxxxxxxxxx

Risk Management: Both standards require risk assessments, but IEC 62443
places a stronger emphasis on operational resilience and the unique challenges of OT environments.

Smart connected Street lighting (IT, OT, & IoT)

Internet of Things

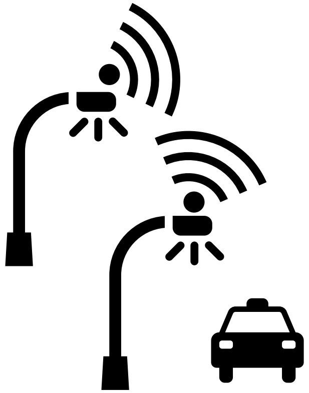
Involves connecting physical streetlights to the internet

- Sensors, Transmitting data to data centers

Operational Technology

Controls physical products including the sensors

- Real time response, use of PLC's



IT, OT & IoT Standards

IoT

- EN 18031 (-1, -2, -3)
- ETSI EN 303 645

IT

- ISO 27001

OT

- IEC 62443 (-4-1, -4-2, -3-3, -2-4)

Different in standard requirements IT & OT

OT: Environments: Require highly specific standards that cater to the unique challenges of industrial processes.

IT: Environments: Need flexible and scalable standards to handle diverse data and network requirements.

IoT: Must navigate both worlds, leveraging the strengths of each set of standards without compromising on security or functionality

Summary for strong cybersecurity you need to have both IT and OT

Thank you!

innovating safety & security

Any questions?