Microsoft

Drivers and Expected Benefits of Composition

Eustace Asanghanwa
Principal PM, IoT Security R&D

Agenda

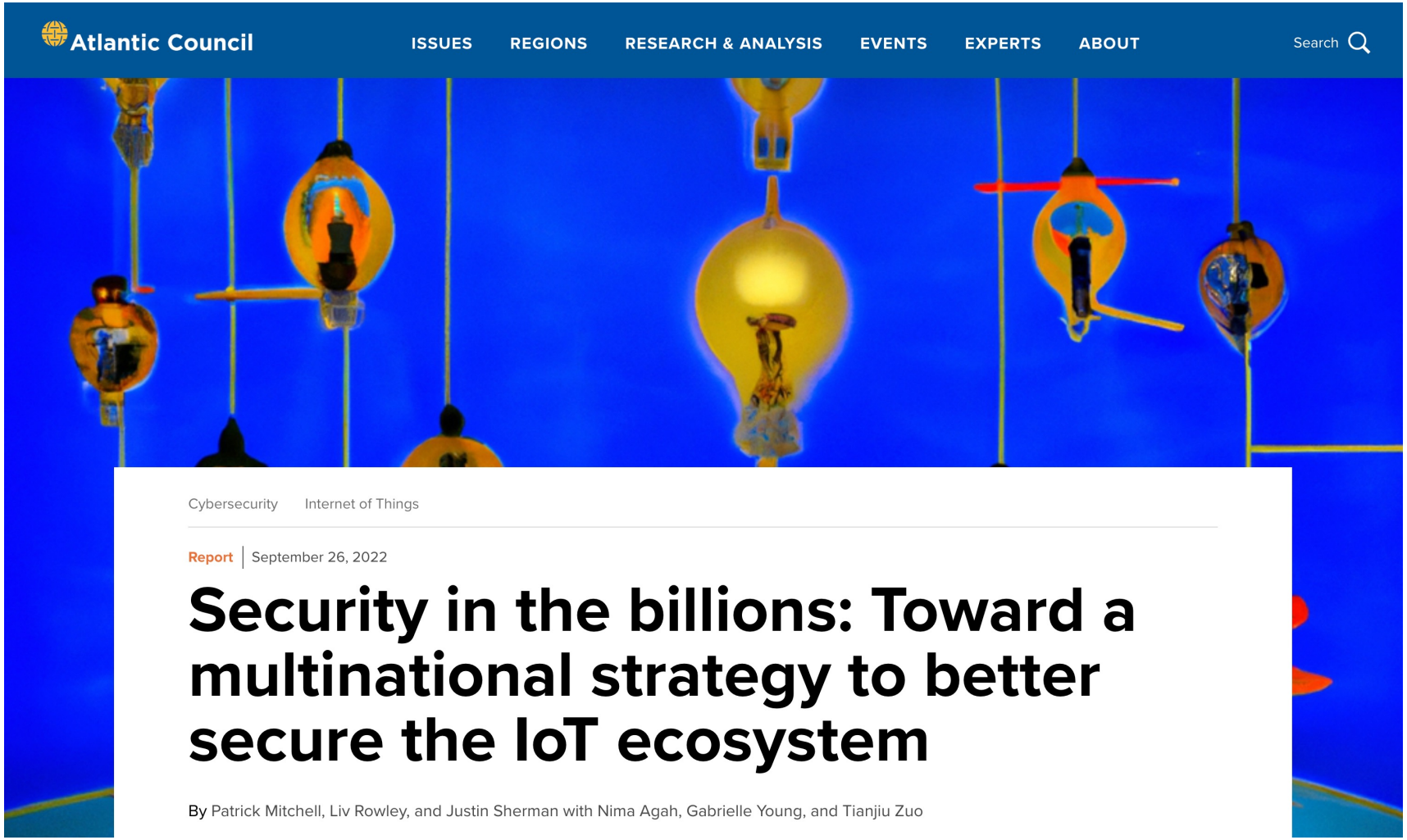
- IoT security – where to apply first?
- Regulatory trends – history predicts future
- Our observations and experience with industries and partners
- Final insights

Agenda

- **IoT security – where to apply first?**
- Regulatory trends – history predicts future
- Our observations and experience with industries and partners
- Final insights

The Atlantic Council

SELF DESCRIPTION: *Driven by our mission of "shaping the global future together," the Atlantic Council is a nonpartisan organization that galvanizes US leadership and engagement in the world, in partnership with allies and partners, to shape solutions to global challenges.*



"...bit consumer focused."

SOURCE: https://www.atlanticcouncil.org/in-depth-research-reports/report/security-in-the-billions

What comes to mind **first** when you think about security for IoT?

Hardly consumer IoT

Critical Infrastructure classifications around the world confirms this

NARY A COMPONENT IN CLASSIFICATIONS FOR CRITICAL INFRASTRUCTURES BY MANY NATIONS - BELOW EXAMPLE FROM US GOVERNMENT SHOWING THE 16 CRITICAL INFRASTRUCTURE SECTORS IN ITS CLASSIFICATION, AND LARGELY SIMILAR IN APPROACH WITH CLASSIFICATIONS FROM OTHER GOVERNMENTS

Chemicals

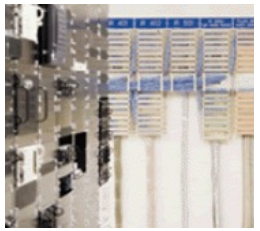
Communica-tions

Dams

Emergency Services

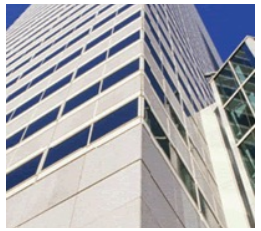
Financial services

Government facilities



Information technology

Transportation Systems



Commercial facilities

Critical manufacturing

Defense Industrial Base

Energy

Food and Agriculture

Healthcare and Public Health

Nuclear Reactors, Materials, and Waste

Water and Wastewater systems

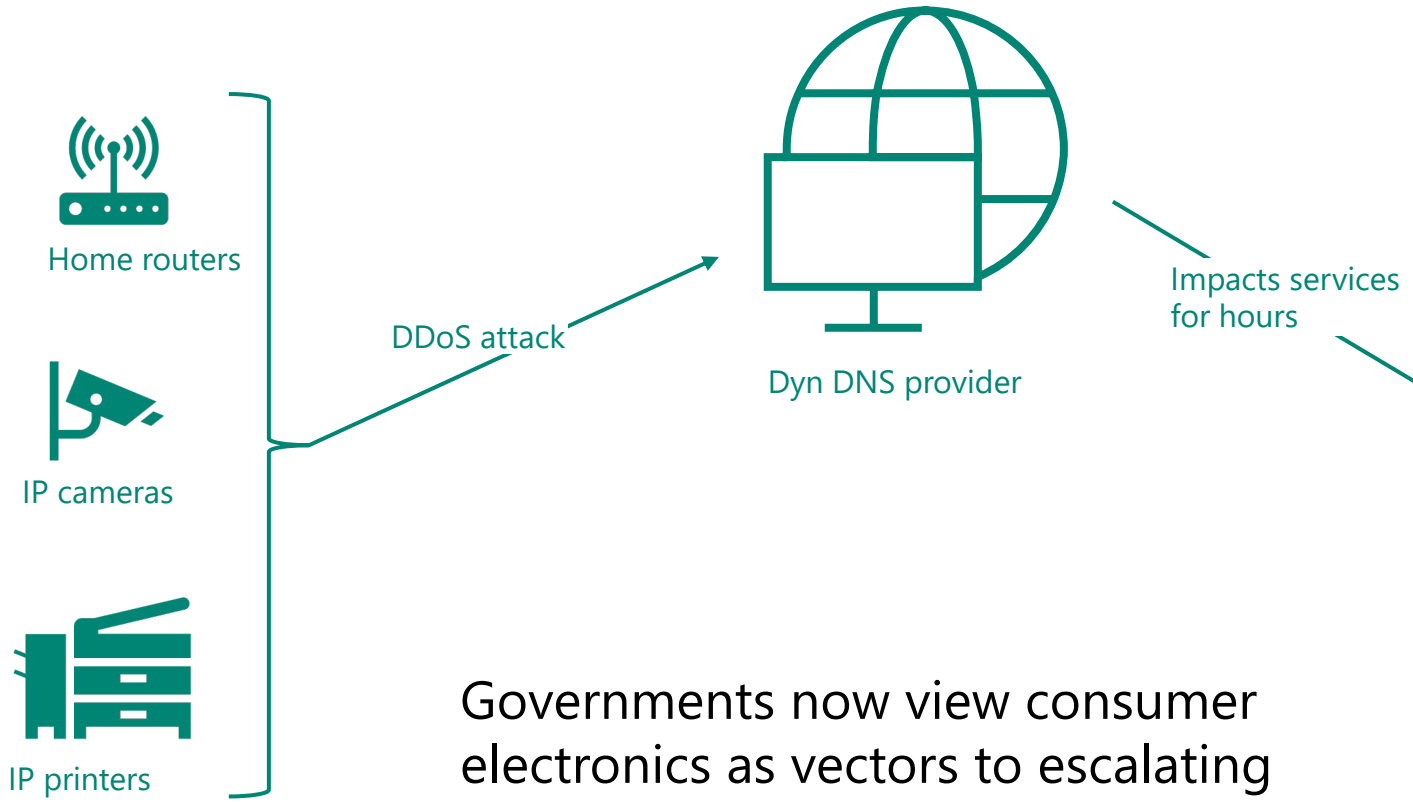
SOURCE: https://www.cisa.gov/critical-infrastructure-sectors

And the logic is on point from everyday experience

	Industrial/Enterprise Electronics	Consumer Electronics
Expected product life	Very long (often > 10 years)	Short (sometimes by design)
Likelihood to invest in security independent of regulations (business/brand motivations)	Very high	Low
Likelihood to implement IoT security standards as risk management strategy	Very high	Low
Likelihood to possess technical savviness for IoT security	Very high	Low
Likelihood for deployments behind safe perimeters and firewalls	Very high	Low
Likelihood to regulatory exposure	Very high	Not likely (but this is changing…)

2016 DDoS Attack on Dyn

Commands attention of US Department of Homeland Security (DHS)



Up to 600K Mirai malware infected consumer electronics

Governments now view consumer electronics as vectors to escalating attacks into critical infrastructure

1. Airbnb
2. Amazon.com
3. Ancestry.com
4. *The A.V. Club*
5. BBC
6. *The Boston Globe*
7. Box
8. *Business Insider*
9. CNN
10. Comcast
11. CrunchBase
12. DirecTV
13. *The Elder Scrolls Online*
14. Electronic Arts
15. Etsy
16. Evergreen ILS
17. FiveThirtyEight
18. Fox News
19. *The Guardian*
20. GitHub
21. Grubhub
22. HBO
23. Heroku
24. HostGator
25. iHeartRadio
26. Imgur
27. Indiegogo
28. Mashable
29. National Hockey League
30. Netflix
31. *The New York Times*
32. Overstock.com
33. PayPal
34. Pinterest
35. Pixlr
36. PlayStation Network
37. Qualtrics
38. Quora
39. Reddit
40. Roblox
41. Ruby Lane
42. *RuneScape*
43. SaneBox
44. Seamless
45. *Second Life*
46. Shopify
47. Slack
48. SoundCloud
49. Squarespace
50. Spotify
51. Starbucks
52. Storify
53. Swedish Civil Contingencies Agency
54. Swedish Government
55. Tumblr
56. Twilio
57. Twitter
58. Verizon Communications
59. Visa
60. Vox Media
61. Walgreens
62. *The Wall Street Journal*
63. Wikia
64. *Wired*
65. Wix.com
66. WWE Network
67. Xbox Live
68. Yammer
69. Yelp
70. Zillow

SOURCE: https://en.wikipedia.org/wiki/DDoS_attacks_on_Dyn

Insights

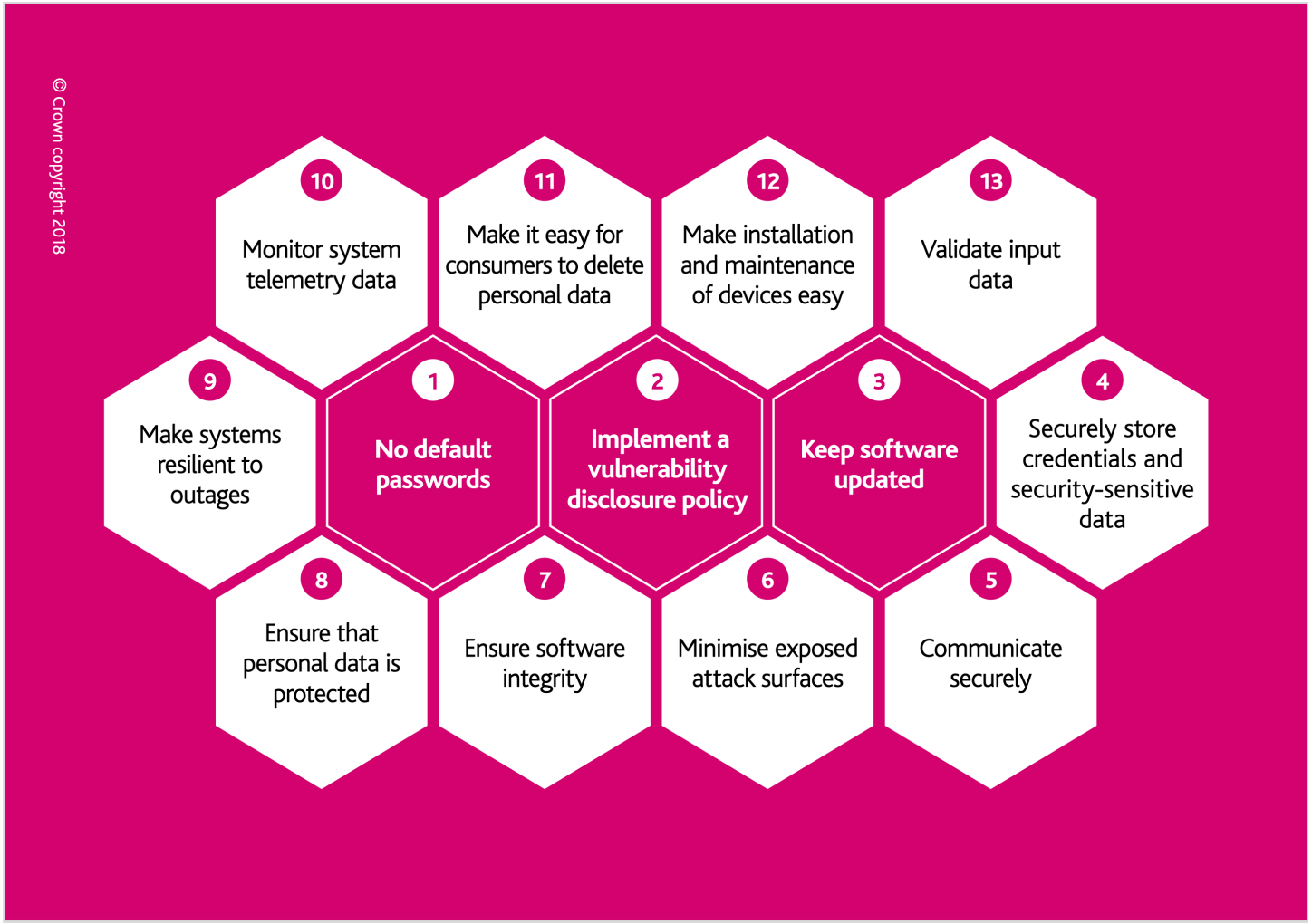
- Consumer electronics are potential vectors for escalated attacks
- Consumer electronics historically weak security posture hence demands greater attention. Governments are noticing.

Agenda

- IoT security – where to apply first?
- **Regulatory trends – history predicts future**
- Our observations and experience with industries and partners
- Final insights

United Kingdom

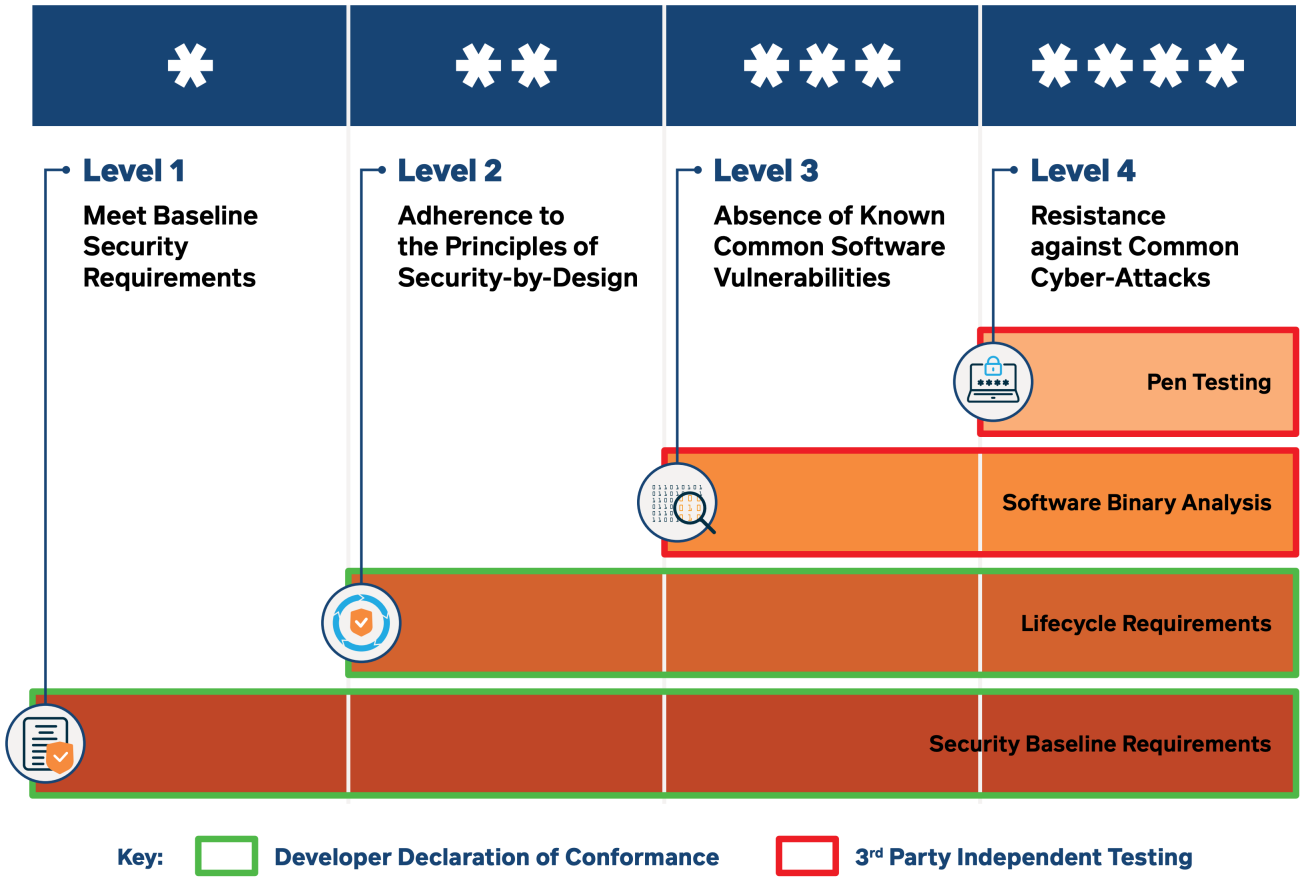
Department for Digital, Culture, Media & Sport



SOURCE: https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security

- ✓ **March 2018** - Published *Secure by Design* report on guidelines for securing consumer IoT.
- ✓ **October 2018** – Published *Thirteen Principles of consumer IoT Security* in coordination with industry. In collaboration with ETSI.
- ✓ Voluntary → low industry uptake.
- ✓ **November 2021** – New Bill (PSTI) empowers DCMS to regulate and enforce mandatory security baselines.
- ✓ Penalties for non-compliance to include fines up to GBP 10M or 4% worldwide revenue, product recalls or outright product bans.

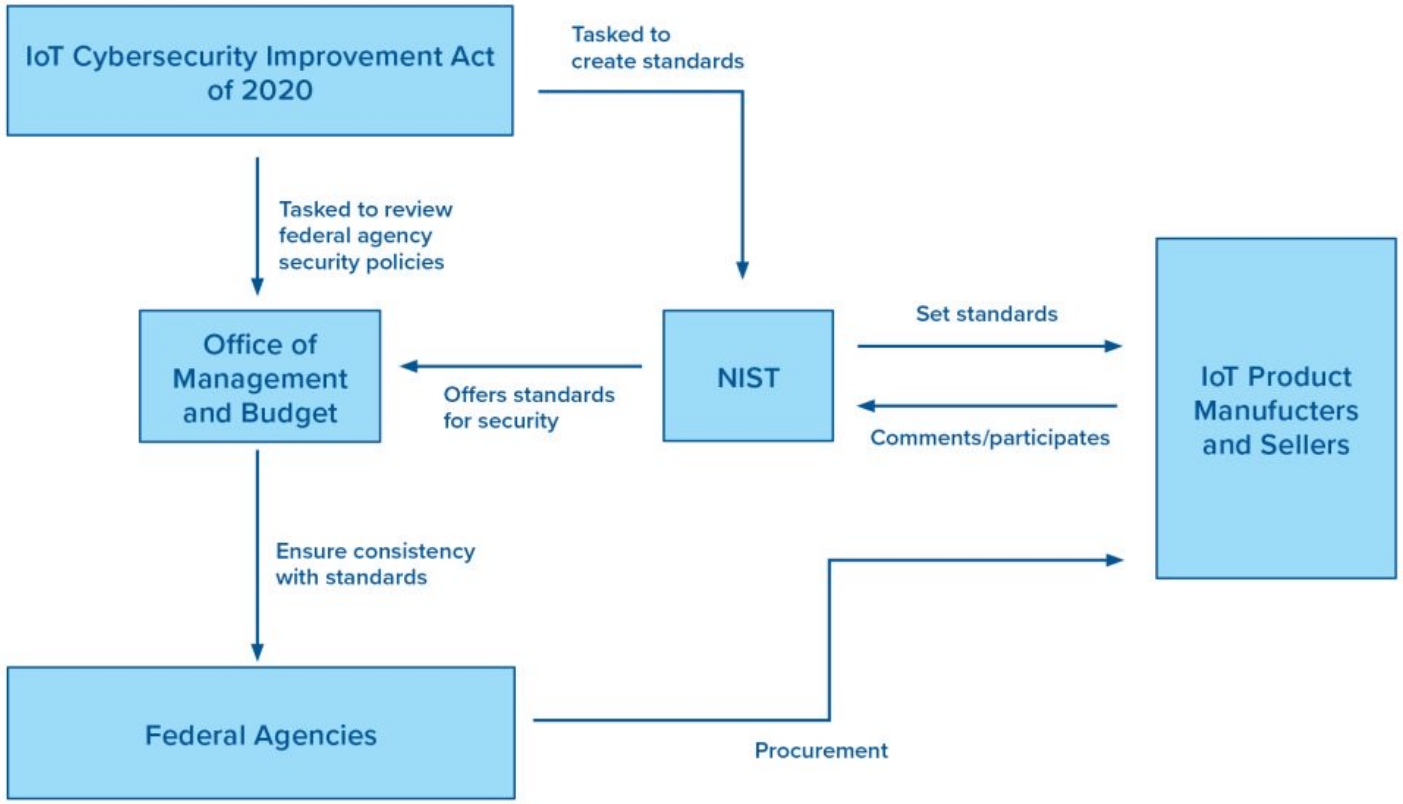
Singapore



- ✓ **October 2020**- Cybersecurity Agency (CSA) launched Cybersecurity labeling scheme (CLS).
- ✓ Voluntary with **mandatory** requirements
  → CLS Level 1 for all new internet routers
  → CLS Level 4 supplemental Minimum Test Specification for contact tracing devices
- ✓ CLS Level 3 & 4 cross-recognition with Finnish scheme telegraphs need for global alignment.

SOURCE: https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/for-manufacturers

United States

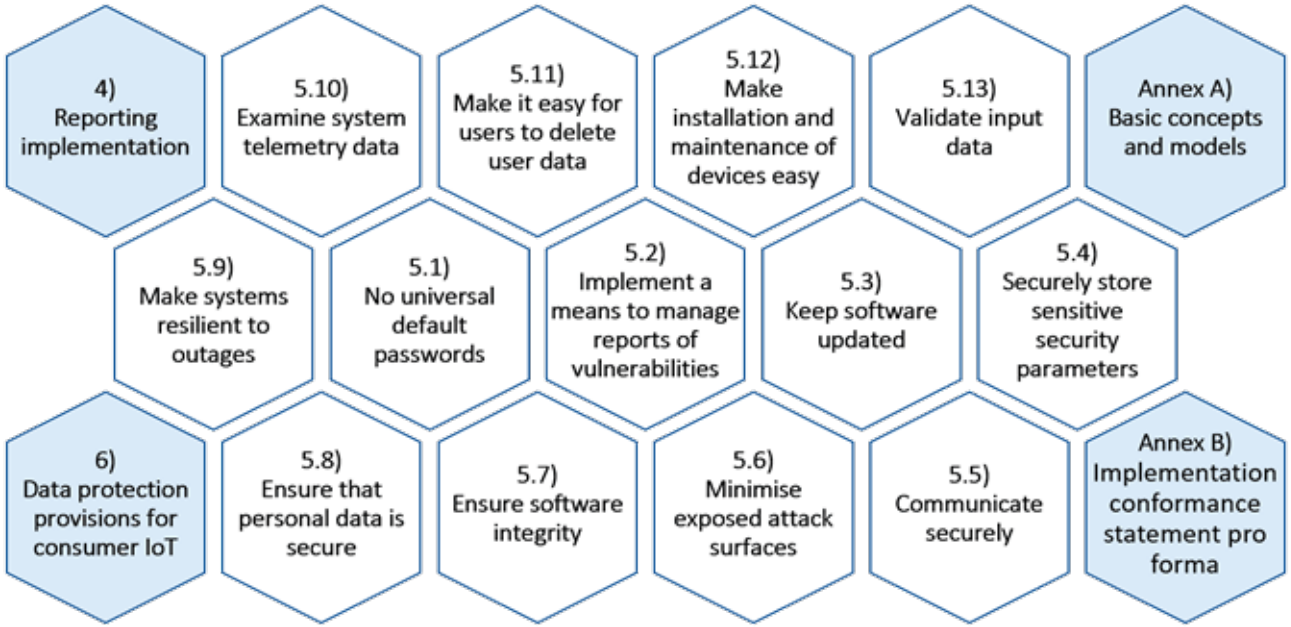


SOURCE: https://www.atlanticcouncil.org/in-depth-research-reports/report/security-in-the-billions/

- ✓ **January 2020**: California Senate Bill SB-327, *Security of Connected Devices* law, went into effect
- ✓ **January 2020**: Oregon House Bill HB 2395 law on securing IoT devices went into effect
- ✓ Voluntary → Low industry uptake
- ✓ **December 2020**: US H.R. 1668, *IoT Cybersecurity Improvement Act of 2020*, became law.
- ✓ **May 2021**: President Biden's *Executive Order EO 14028 of May 12, 2021, Improving the nation's cybersecurity.* Includes call to create "energy star" like label program and *incentivize* manufacturers.

Australia

Australian Government
Department of Home Affairs



- ✓ **August 2020**: Released *Code of Practice: Securing the Internet of Things for Consumers*. Influenced by thirteen principles from ETSI EN 303 645
- ✓ Voluntary → Low industry uptake.
- ✓ Signaled intent to regulate with fines and penalties for non-compliance. Up to all thirteen principles potentially in play for a minimum baseline.

SOURCE: https://www.etsi.org/technologies/consumer-iot-security

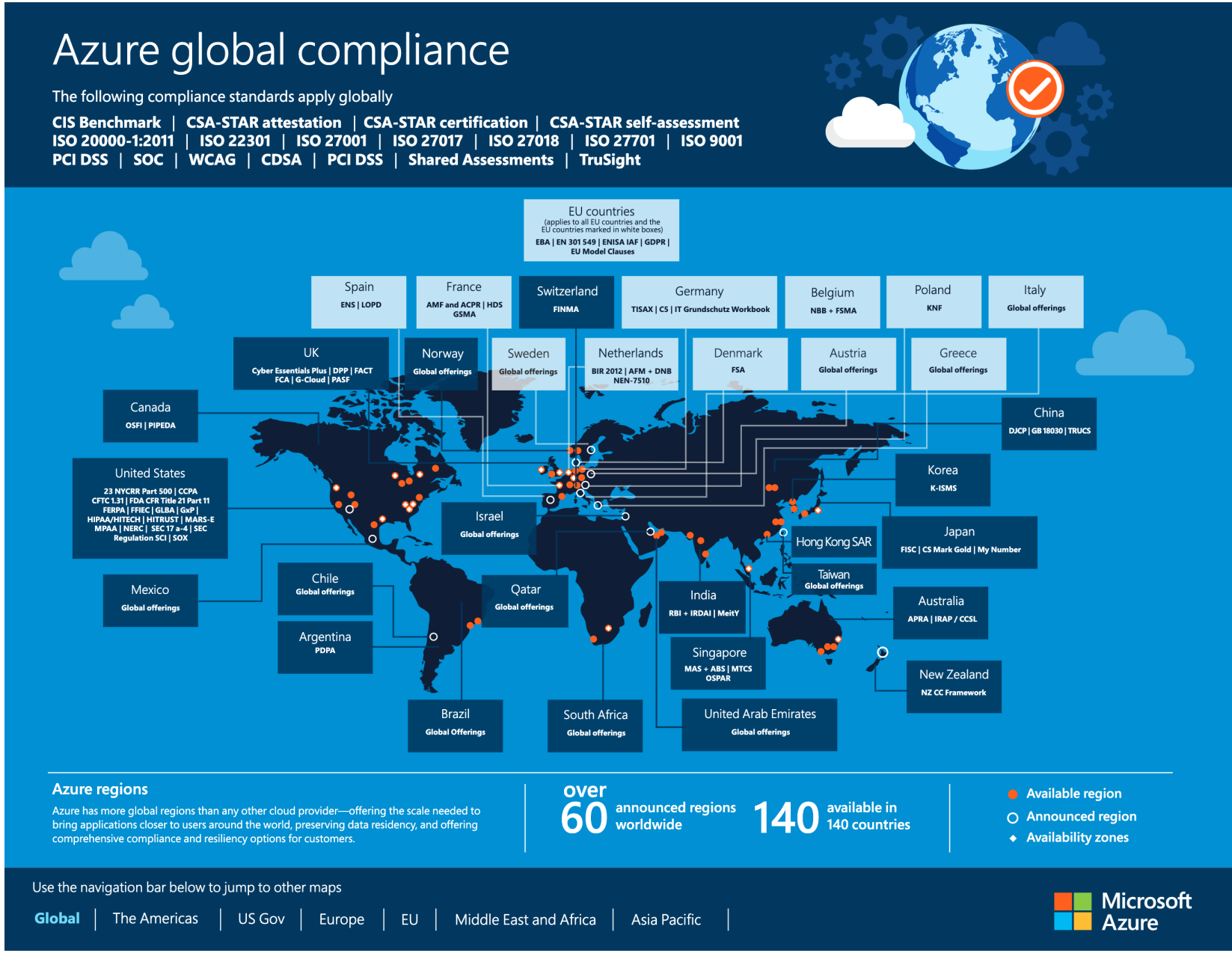
Insights

- Consumer electronics are potential vectors for escalated attacks
- Consumer electronics historically weak security posture hence demands greater attention. Governments are noticing.
- Governments are staging for regulation of IoT security that is backed by heavy fines and penalties for non-compliance
- Heavy focus on consumer electronics where maturity in security practices is at infancy hence a heightened threat potential

Agenda

- IoT security – where to apply first?
- Regulatory trends – history predicts future
- **Our observations and experience with industries and partners**
- Final insights

Azure has more global regions than any other cloud provider



SOURCE: https://www.microsoft.com/trust-center

Currently over 110 compliance offerings on Microsoft Azure

THE MOST BY ANY CLOUD PROVIDER - A STRONG COMMITMENT TO THE SUCCESS OF ALL BUILDING ON AZURE

Global
- CIS benchmark
- CSA STAR Attestation
- CSA STAR Certification
- CSA STAR self-assessment
- SOC 1
- SOC 2
- SOC 3

Global
- ISO 20000-1
- ISO 22301
- ISO 27001
- ISO 27017
- ISO 27018
- ISO 27701
- ISO 9001
- WCAG

US government
- CJIS
- CMMC
- CNSSI 1253
- DFARS
- DoD IL2
- DoD IL4
- DoD IL5
- DoD IL6
- DoE 10 CFR Part 810
- EAR
- FedRAMP
- FIPS 140

US government
- ICD 503
- IRS 1075
- ITAR
- JSIG
- NDAA
- NIST 800-161
- NIST 800-171
- NIST 800-53
- NIST 800-63
- NIST CSF
- Section 508 VPATs
- StateRAMP

Financial services
- 23 NYCRR Part 500 (US)
- AFM and DNB (Netherlands)
- AMF and ACPR (France)
- APRA (Australia)
- CFTC 1.31 (US)
- EBA (EU)
- FCA and PRA (UK)
- FFIEC (US)
- FINMA (Switzerland)

Financial services
- FINRA 4511 (US)
- FISC (Japan)
- FSA (Denmark)
- GLBA (US)
- KNF (Poland)
- MAS and ABS (Singapore)
- NBB and FSMA (Belgium)
- OSFI (Canada)

Financial services
- OSPAR (Singapore)
- PCI 3DS
- PCI DSS
- RBI and IRDAI (India)
- SEC 17a-4 (US)
- SEC Regulation SCI (US)
- SOX (US)
- TruSight

Healthcare and life sciences
- ASIP HDS (France)
- EPCS (US)
- GxP (FDA 21 CFR Part 11)
- HIPAA (US)
- HITRUST
- MARS-E (US)
- NEN 7510 (Netherlands)

Automotive, education, energy, media, and telecommunication
- CDSA
- DPP (UK)
- FACT (UK)
- FERPA (US)
- MPA
- GSMA
- NERC (US)
- TISAX

Regional - Americas
- Argentina PDPA
- Canada privacy laws
- Canada Protected B
- US CCPA

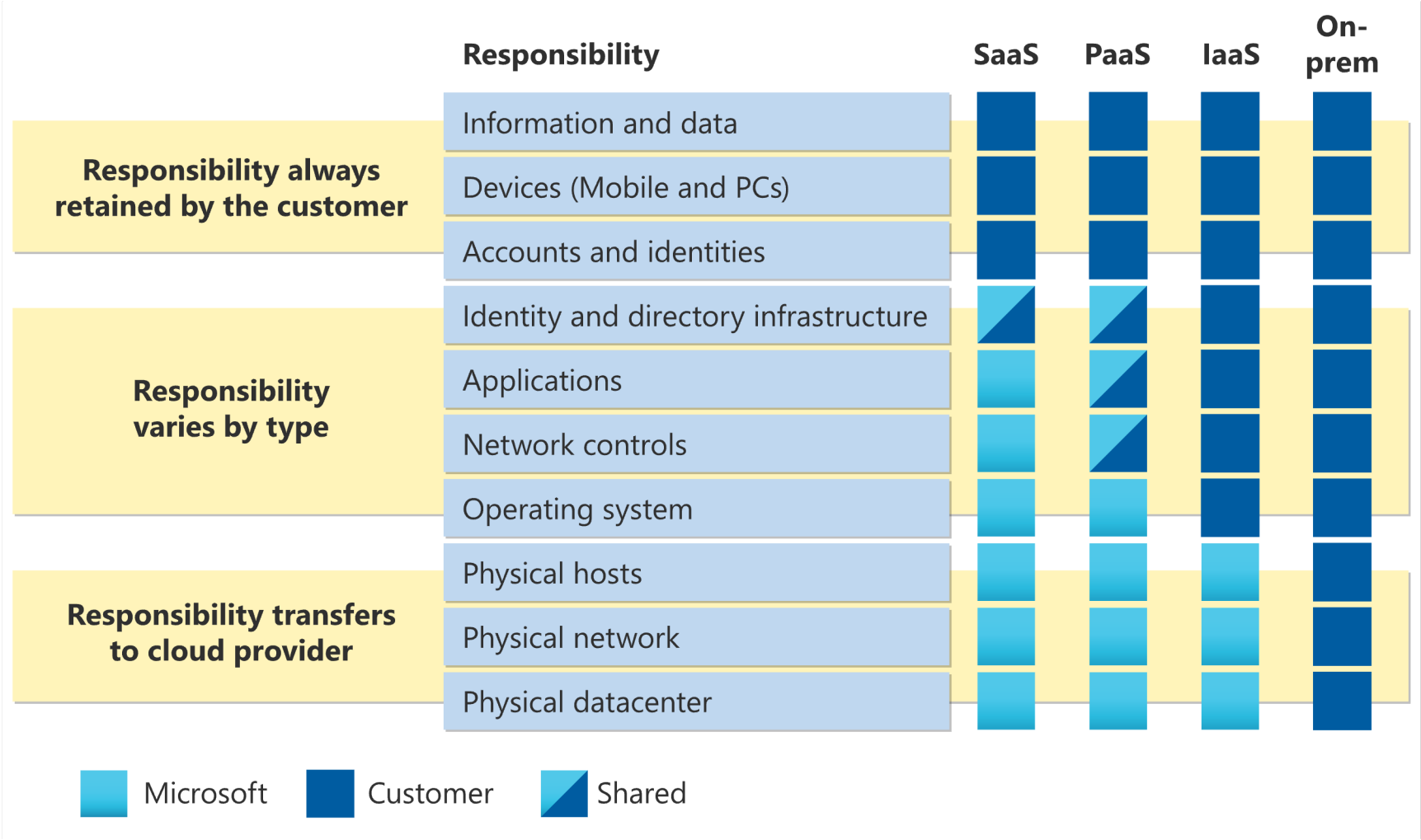
Regional - EMEA
- Russia personal data law
- Spain ENS High
- Spain LOPD
- UAE DESC
- UK Cyber Essentials Plus
- UK G-Cloud
- UK PASF

Regional - EMEA
- EU Cloud CoC
- EU EN 301 549
- ENISA IAF
- EU GDPR
- EU Model Clauses
- Germany C5
- Germany IT-Grundschutz workbook
- Netherlands BIR 2012
- Qatar NIA

Regional - Asia Pacific
- Australia IRAP
- China GB 18030
- China DJCP (MLPS)
- China TCS
- India MeitY
- Japan CS Gold Mark
- Japan ISMAP
- Japan My Number Act
- Korea K-ISMS
- New Zealand ISPC
- Singapore MTCS

SOURCE: https://www.microsoft.com/trust-center

Compliance is always a shared responsibility



SOURCE: https://www.microsoft.com/trust-center

How it could have happened...

Willow TrustBox Edge Gateway

A small & secure device that is both quick & easy to deploy, for network protocol connectors to stream live to the WillowTwin™.

- ✓ Hosts Willow protocol connectors
- ✓ Powered by Microsoft Azure IoTEdge
- ✓ Securely hardened, protected & actively monitored — ECN PP
- ✓ Remotely managed with outbound only communication
- ✓ GDPR, CIS & NIST compliant — SESIP

Scalys Microsoft

IoT Signals 2022: Manufacturing as leading Indicator

Discrete, hybrid, and process manufacturing

Exhibit 2.4: Companies look to OEMs for smart factory support most often

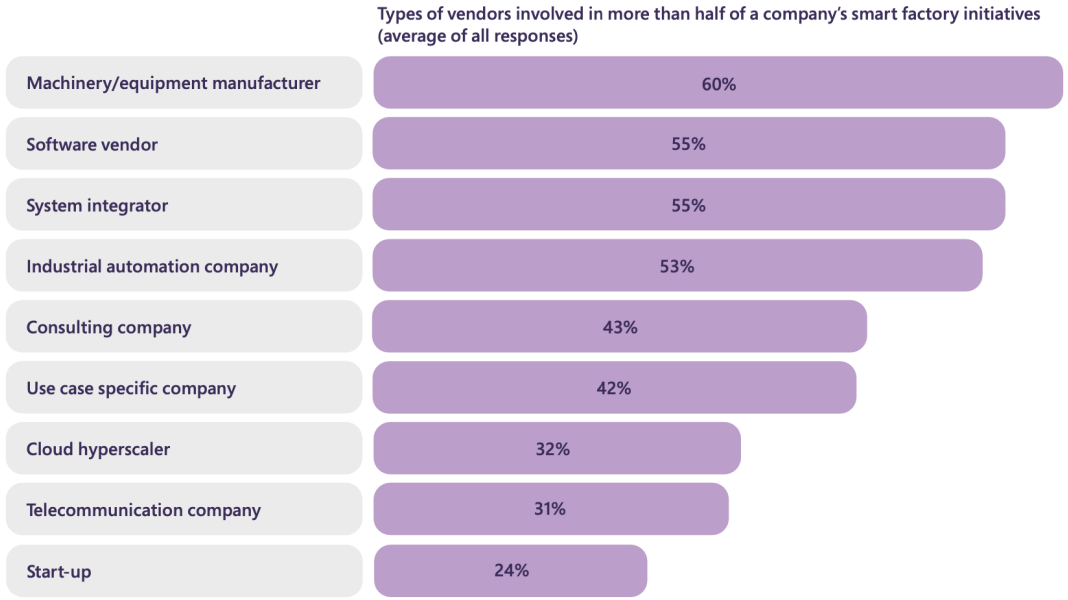
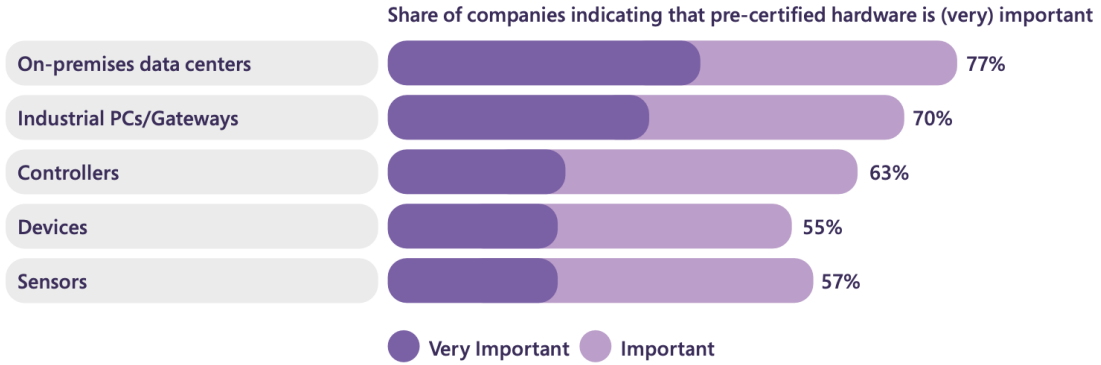


Exhibit 6.7: Companies want pre-certified edge computing hardware



Get the full report:
https://info.microsoft.com/ww-landing-IoT-signals-manufacturing-spotlight.html

Azure RTOS positioned for compliance

PRE-CERTIFIED AND CERTIFIED FOR NUMEROUS SAFETY AND SECURITY STANDARDS

IEC 61508 SIL4
Functional safety – all industries

IEC 62304 SW Class C
Medical devices

ISO 26262 ASIL D
Automotive applications

EN 50128 SIL4
Railway applications

UL/IEC 60730 – 1 Class B
Household electrical devices

UL/IEC 60335 – 1 Class B
Home appliances

UL/IEC 60335 – 1 Class B
Home appliances

SESIP™
(Level 3 - ongoing)

psacertified™
level one

The Common Criteria *Edge Compute Node Protection Profile (ECN PP)*

INDUSTRY STANDARDS DRIVEN HOLISTIC DEVICE SECURITY BASELINE AT THE APPLIANCE LEVEL, ENVISIONS WHOLE SOLUTION COMPLIANCE

In collaboration with industry experts

Scalys Security at the edge

PROVE & RUN

SGS brightsight

arm

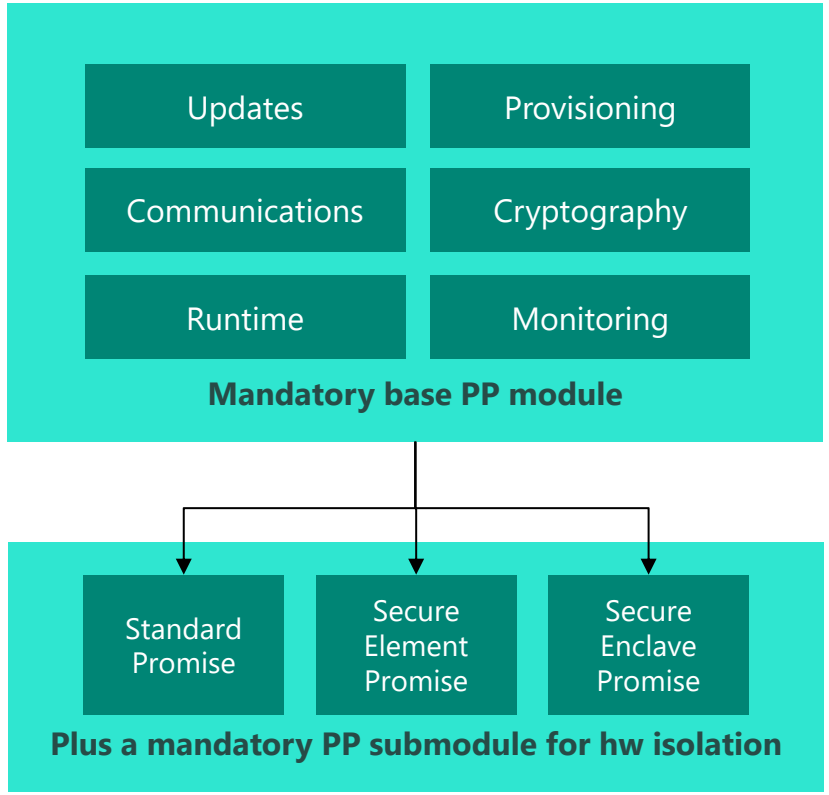
NXP

TÜVRheinland®

TRUSTCB

riscure

UL



Base PP + PP submodule provides holistic security baseline claim for the edge compute node

Security hardening roots of trust subject to relevant certifications such as PSACertified™, SESIP, FIPS 140

Reference: https://aka.ms/ecn-pp

And we're really excited about ECN PP and SESIP mapping by GlobalPlatform SESIP Sub Task force

Mapping Edge Computing Standards to SESIP

BACK TO ALL BLOGS

By Carlos Serratos, SGS Brightsight

The objective of developers of Internet of Things (IoT) devices is to bring to market products that aim to operate a specific use case (home appliance, automotive, industrial, entertainment, etc.). When this use case does not have a security or safety purpose, developers focus more on functionality, usability, and performance than on security, a domain in

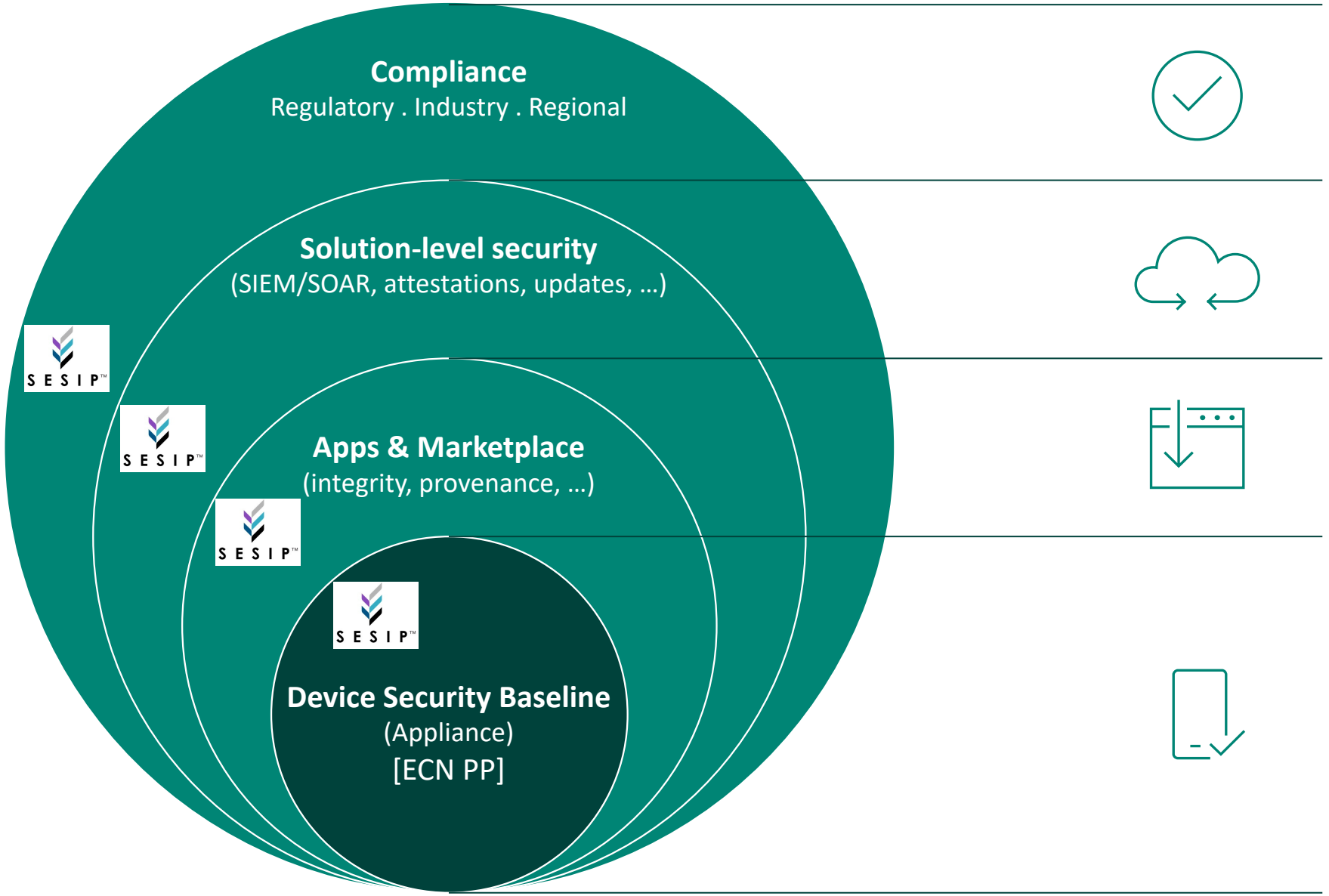
Share This

LATEST NEWS
NEWSLETTER
BLOG
INDUSTRY EVENTS
MEDIA AND ANALYST KIT

The GlobalPlatform SESIP Sub Task force has undertaken the mapping between **ECN PP** and SESIP. The drivers and expected benefits of this work item are around two forms of composition:

- Lower composition, provides a path for making use of SESIP certified components and platforms for showing readiness towards this PP, reducing the effort for developers looking to achieve ECN PP certifications under CC
- Upper composition, as the mapping of the ECN PP using SESIP can be linked towards other standards like 62443, while maintaining the CC trust mark.

SESIP as streamlined tactical pathway ECN PP compliance at every layer



Agenda

- IoT security – where to apply first?
- Regulatory trends – history predicts future
- Our observations and experience with industries and partners
- **Final insights**

Final Insights

- Consumer electronics are potential vectors for escalated attacks
- Consumer electronics historically weak security posture demands greater attention
- Governments are staging for regulatory oversights into IoT security with fines and penalties for non-compliance
- Governments are consumer electronics where maturity in security practices is at infancy
- Device Manufacturers are most exposed to compliance fragmentation and are increasingly on the hook for compliance by solution builders.
- We see SESIP's *divide-and-conquer-through-composition* approach to device security compliance as the most expedient path forward
- Because of the shared responsibility model to compliance, we can't solve it all but are still committed to the success of our partners. SESIP certification for Azure RTOS and Edge Compute Node Protection Profile(ECN PP) are just examples

Conclusion

So, what are *The drivers and expected benefits of composition?*

- **Driver**: New emphasis on consumer electronics – more to comply
- **Driver**: Compliance fragmentation across governments – more to certify
- **Driver**: Velocity of change from voluntary to regulation – penalties
- **Driver**: Compliance cross-recognition programs – program reach
- **Driver**: Manufacturer compliance exposure – access more markets
- **Benefit**: Scale device compliance across regulatory regions
- **Benefit**: Scale device compliance support across industry verticals
- **Benefit**: Lower certification burden and costs with piecemeal compliance

For more info, check out topic specific links provided in respective slides

Microsoft

Thank you