



HOW TO GET READY FOR A WORLD OF IoT CYBER SECURITY REGULATIONS?

Dr. Cédric LEVY-BENCHETON

@CetomeLtd
cetome.com

CETOME:YOUR IoT CYBER SECURITY CONSULTANCY

**We make IoT Cyber
Security work for you!**

Accelerate project delivery with security-by-design

Keep your products secure after release

Upskill your staff with training and awareness

Consolidate market access in light of regulations

SUMMARY

Why is IoT security still a joke in 2021?

Panorama of IoT Cyber Security Regulations

How to succeed in a world of IoT regulations?

Discussion on the future and conclusions



WHY IS IoT SECURITY STILL A JOKE IN 2021?

DO YOU KNOW...

#IoTSecurity

#RegulateVendors

What the S in IoT stands for?

DO YOU KNOW...

#IoTSecurity

#RegulateVendors

**What the S in IoT
stands for?**

It stands for:

DO YOU KNOW...

#IoTSecurity

#RegulateVendors

**What the S in IoT
stands for?**

It stands for:

**“Stop making the same old
joke, it’s not funny anymore”.**

IoT SECURITY IS NOT A JOKE

Think of the children!

#IoTSecurity

#RegulateVendors



Man hacks Ring camera in 8-year-old girl's bedroom, taunts her: 'I'm Santa Claus'

The hacker also played music and told the girl to mess up her room and break her television.



IoT SECURITY IS NOT A JOKE

Think of our safety!

#IoTSecurity

#RegulateVendors

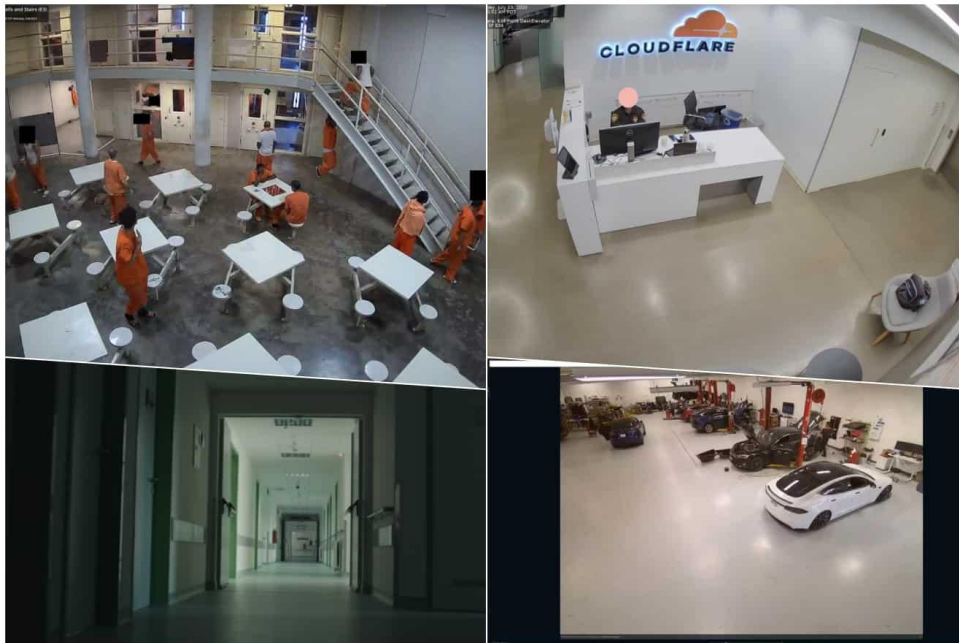


IoT SECURITY IS NOT A JOKE

Think of our privacy!

#IoTSecurity

#RegulateVendors



IoT SECURITY IS NOT A JOKE

#IoTSecurity

Think of our developers and product manufacturers!

#RegulateVendors



Services ▾ Resource Groups ▾

Personal Health Dashboard

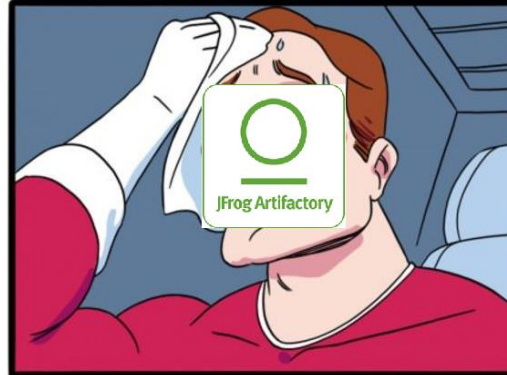
Dashboard

Event log

Event log

Filter by tags or attributes

Event	Status
<input type="radio"/> Datapipeline operational issue	Open
<input type="radio"/> Elasticbeanstalk operational issue	Closed
<input type="radio"/> Workmail operational issue	Closed
<input type="radio"/> ECR operational issue	Closed
<input type="radio"/> Elastictranscoder operational issue	Closed
<input type="radio"/> ACM operational issue	Closed
<input type="radio"/> S3 operational issue	Closed
<input type="radio"/> Mobilehub operational issue	Closed
<input type="radio"/> Firehose operational issue	Closed
<input type="radio"/> KMS operational issue	Closed
<input type="radio"/> Redshift operational issue	Closed
<input type="radio"/> Elasticfilesystem operational issue	Closed
<input type="radio"/> Glacier operational issue	Closed
<input type="radio"/> Cloudformation operational issue	Open
<input type="radio"/> Elasticmapreduce operational issue	Open
<input type="radio"/> Workspaces operational issue	Open
<input type="radio"/> Storagegateway operational issue	Open



```
GNU nano 2.9.3      laurens — root@sdf flasher: /mnt/home/pi/vpnclient —
                                vpn_client.config

Software Configuration File
#
# You may edit this file when the VPN Server / Client / Bridge program is not running.
#
# In prior to edit this file manually by your text editor,
# shutdown the VPN Server / Client / Bridge background service.
# Otherwise, all changes will be lost.
#
declare root
(
    bool DisableRelayServer false
    bool DontSavePassword false
    bool EnableVPNGateService false
    byte EncryptedPassword
    bool HideVPNGateServiceMessage false
    bool PasswordRemoteOnly false
    string UserAgent Mozilla/5.0$20(Windows$20NT$206.3;$20WOW64;$20rv:29.0)$20Gecko/2
    uint UseSecureDeviceId 0
)
```

```
function s3(tablename, tabledata, successCallback, errorCallback) {
    var bucketName = "static-skypixel-dbeta-me";
    AWS.config.update({
        accessKeyId: 'AKIAIRKNYFZBHSS2COTA',
        secretAccessKey: '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',
        region: 'us-west-2',
        bucket: bucketName
    });
}
```



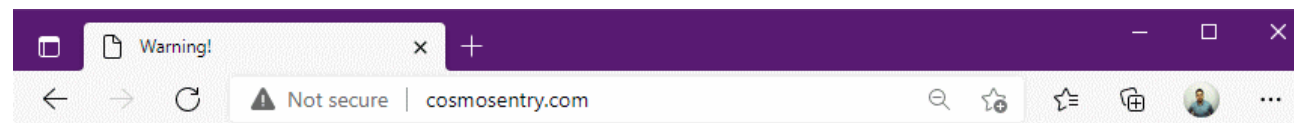
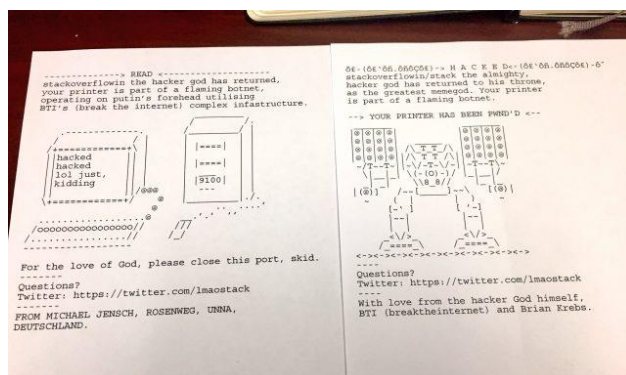
IoT SECURITY IS NOT A JOKE

Think of our digital economy!

#IoTSecurity

#RegulateVendors

root:admin	admin:password
admin:admin	root:root
root:888888	root:12345
root:default	user:user
root:123456	root:pass
root:54321	admin:admin1234
support:support	root:1111
root:	admin:1111
admin:	root:666666



Warning!

Your Mikrotik device is probably infected with Mēris malware, which connects to this domain automatically. We strongly recommend to check your device for viruses or contact your system administrator. Information on how to clean you device is available here <https://blog.mikrotik.com/security/meris-botnet.html>

© Solar JSOC CERT



WELL ACTUALLY!

#IoTSecurity

#RegulateVendors

**IoT Security is still
a joke in 2021**

And no one is laughing

HOW DO WE SECURE IoT?

#IoTSecurity

#RegulateVendors

Don't buy IoT!

HOW DO WE SECURE IoT?

#IoTSecurity
#RegulateVendors

Don't buy IoT!

Change your password!

HOW DO WE SECURE IoT?

#IoTSecurity

#RegulateVendors

Don't buy IoT!

Change your password!

Patch your devices!

HOW DO WE SECURE IoT?

#IoTSecurity

#RegulateVendors

Don't buy IoT!

Change your password!

Patch your devices!

Use MFA!

HOW DO WE SECURE IoT?

#IoTSecurity

#RegulateVendors

Don't buy IoT!

Patch your devices!

Change your password!

Use MFA!

Get a VPN!

HOW DO WE SECURE IoT?

#IoTSecurity

#RegulateVendors

Don't buy IoT!

Change your password!

Patch your devices!

Use MFA!

Get a VPN!

Use a dedicated network!

HOW DO WE SECURE IoT?

#IoTSecurity

#RegulateVendors

Don't buy IoT!

Change your password!

Patch your devices!

Use MFA!

Get a VPN!

Use a dedicated network!

BLCOKHCAIN!11!

HOW DO WE SECURE IoT?

#IoTSecurity

#RegulateVendors

STOP

Don't buy IoT! Change password!
Patch your devices! Use MFA Get a VPN
Use a dedicated network! COINCAIN!11



PANORAMA OF IoT CYBER SECURITY REGULATIONS

WHY DO WE NEED REGULATION?

#IoTRegulations
#RegulateVendors

**Stop blaming
end users!**

WHY DO WE NEED REGULATION?

#IoTRegulations
#RegulateVendors

**Stop blaming
end users!**

**Address the
root causes of
IoT insecurity**

WHY DO WE NEED REGULATION?

#IoTRegulations
#RegulateVendors

**Stop blaming
end users!**

**Address the
root causes of
IoT insecurity**

**Nudge
corporate
investments**

WHY DO WE NEED REGULATION?

#IoTRegulations
#RegulateVendors

**Stop blaming
end users!**

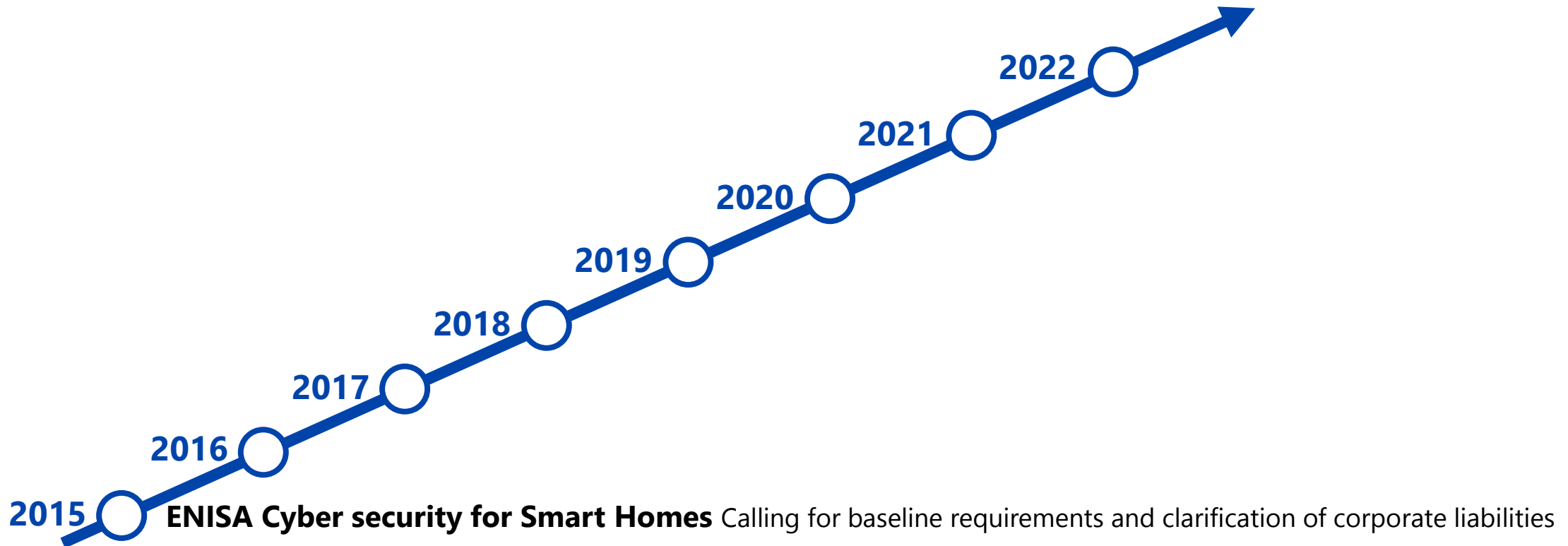
**Address the
root causes of
IoT insecurity**

**Nudge
corporate
investments**

**Clarify “best
practices”**

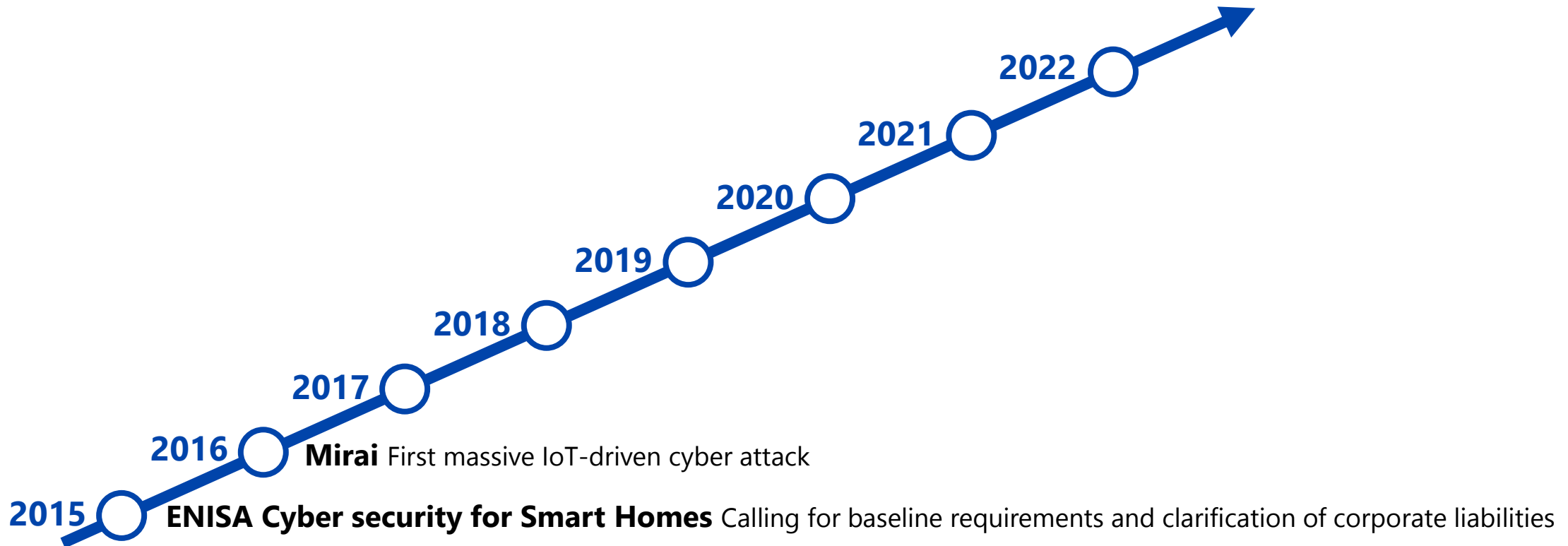
WHY IS REGULATION UNAVOIDABLE?

#IoTRegulations
#RegulateVendors



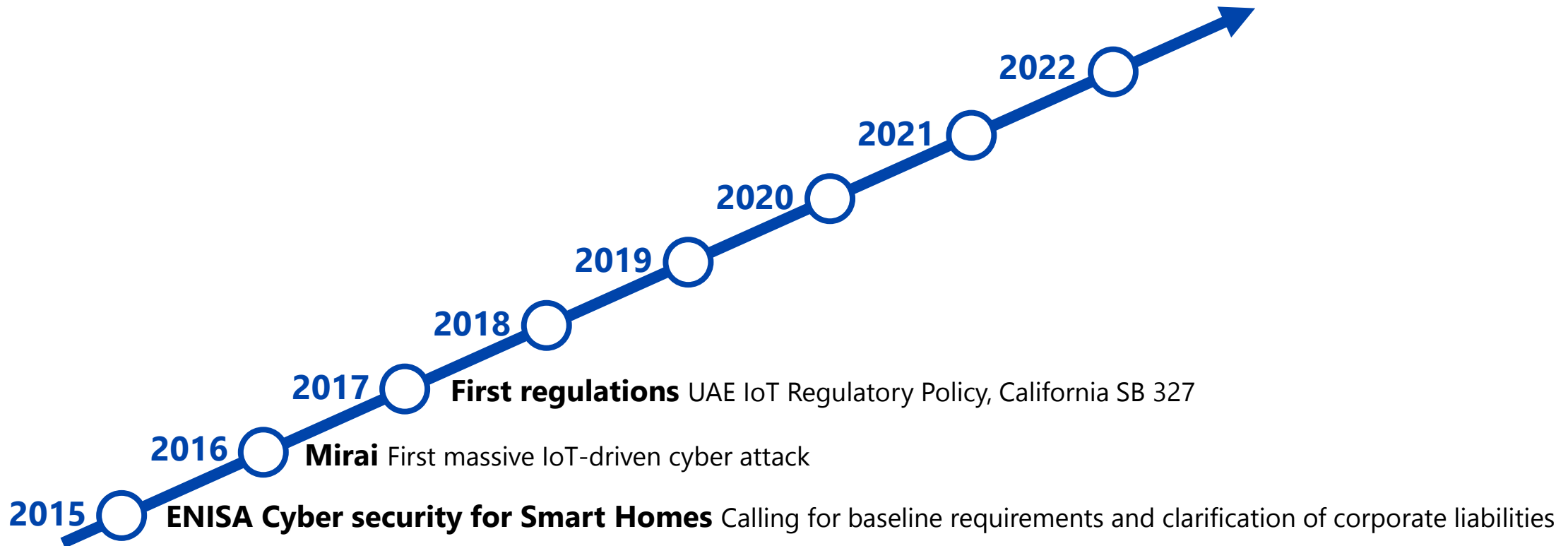
WHY IS REGULATION UNAVOIDABLE?

#IoTRegulations
#RegulateVendors



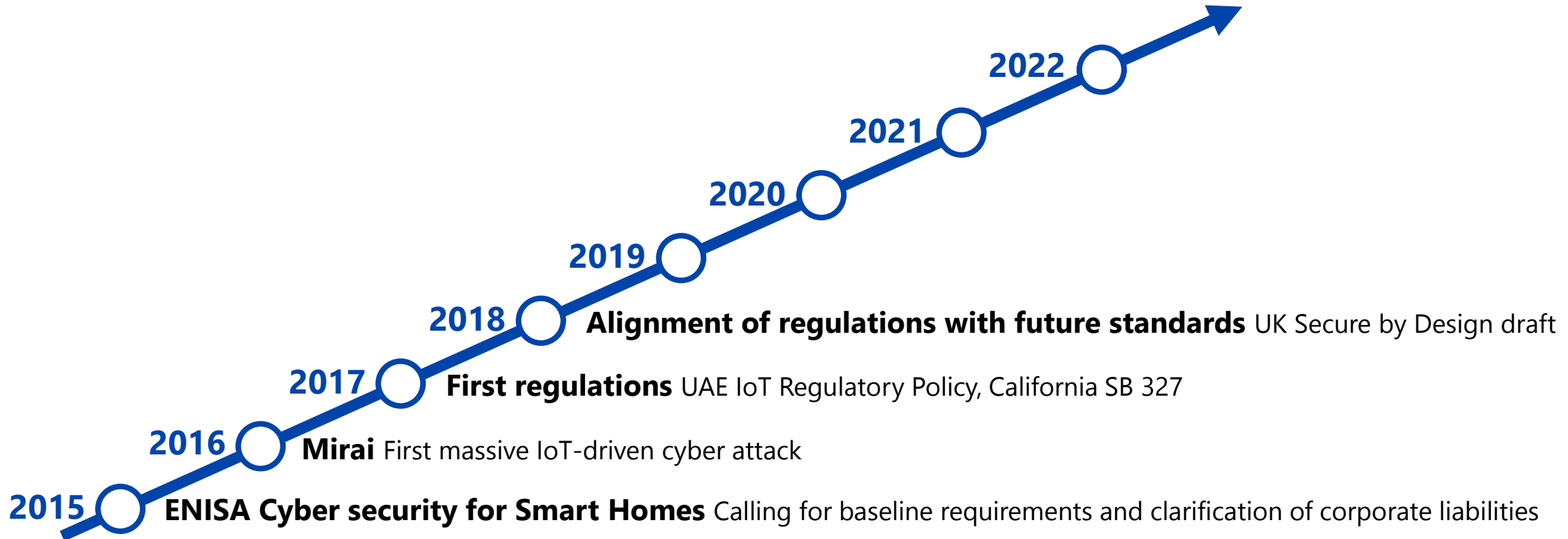
WHY IS REGULATION UNAVOIDABLE?

#IoTRegulations
#RegulateVendors



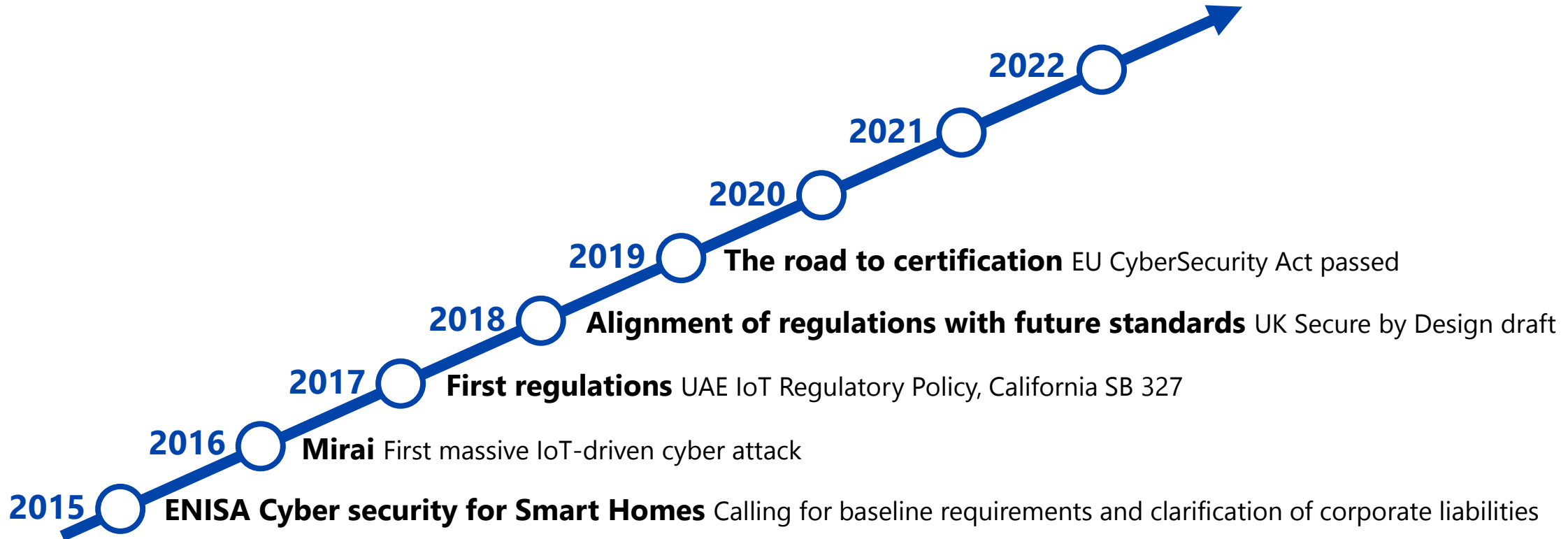
WHY IS REGULATION UNAVOIDABLE?

#IoTRegulations
#RegulateVendors



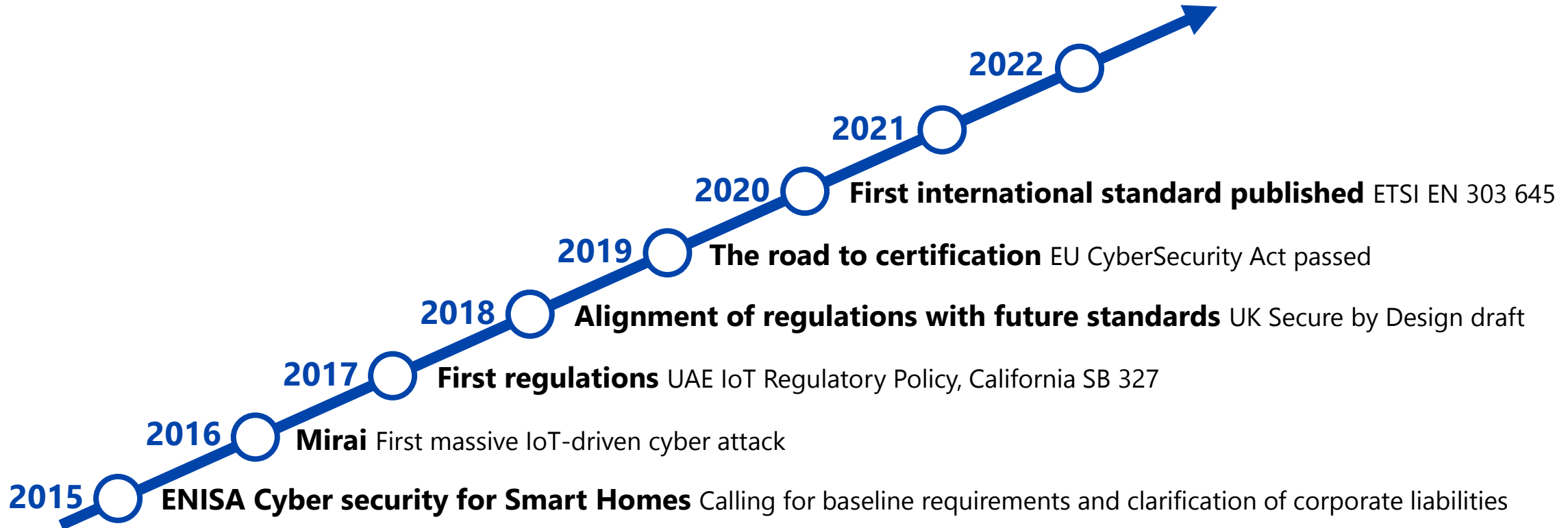
WHY IS REGULATION UNAVOIDABLE?

#IoTRegulations
#RegulateVendors



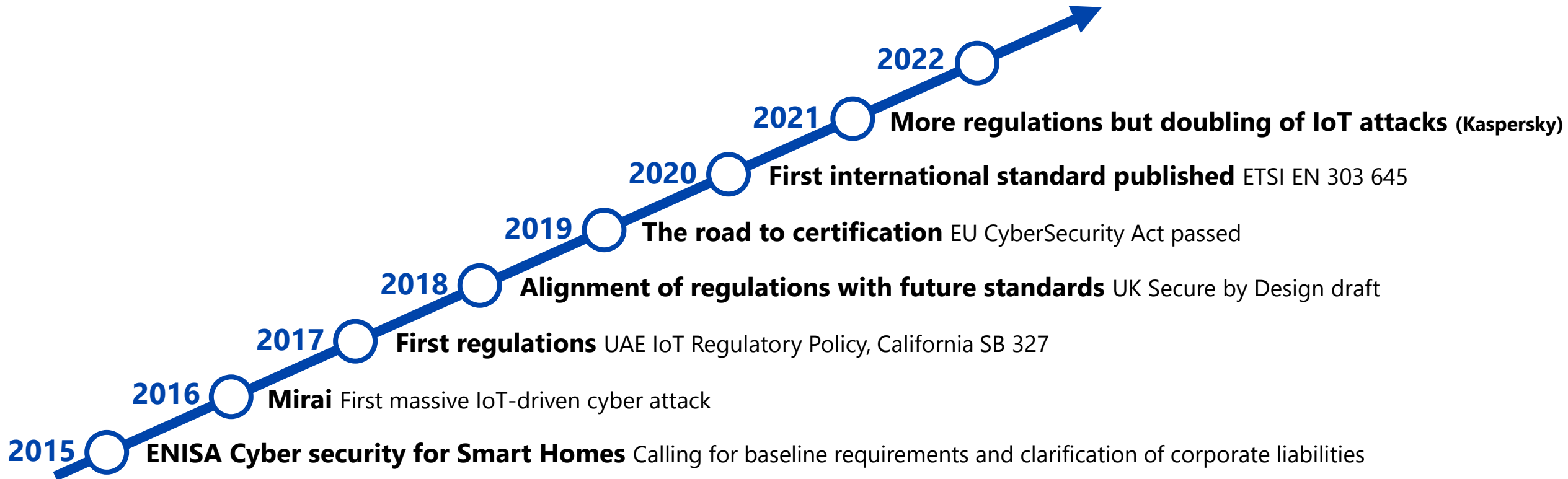
WHY IS REGULATION UNAVOIDABLE?

#IoTRegulations
#RegulateVendors



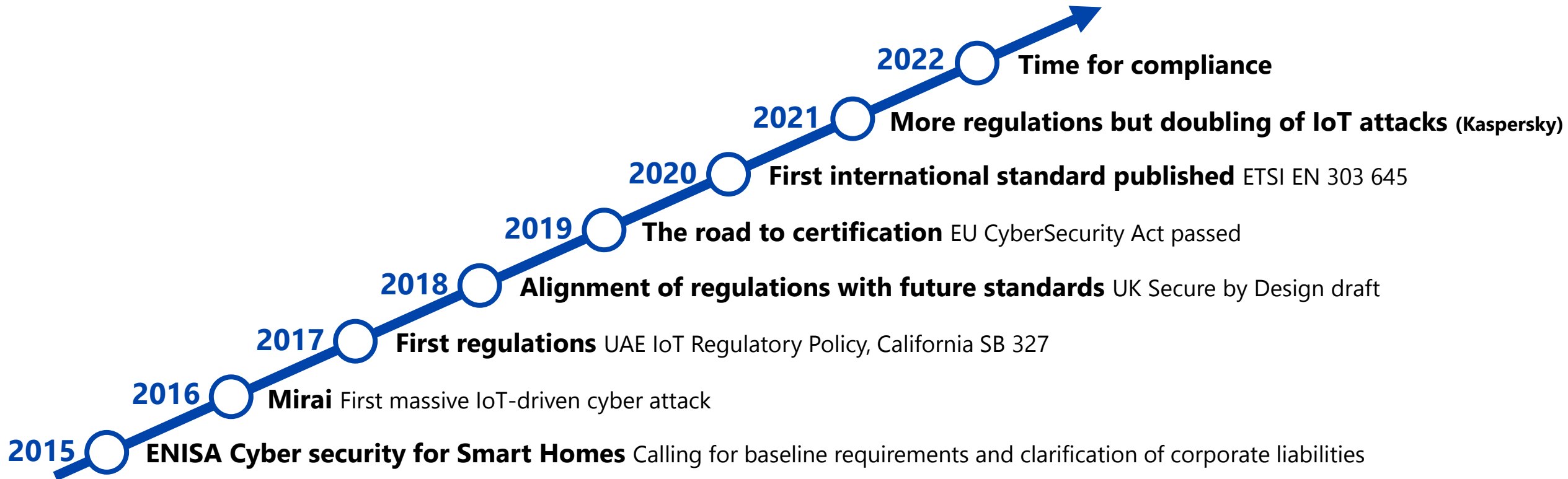
WHY IS REGULATION UNAVOIDABLE?

#IoTRegulations
#RegulateVendors



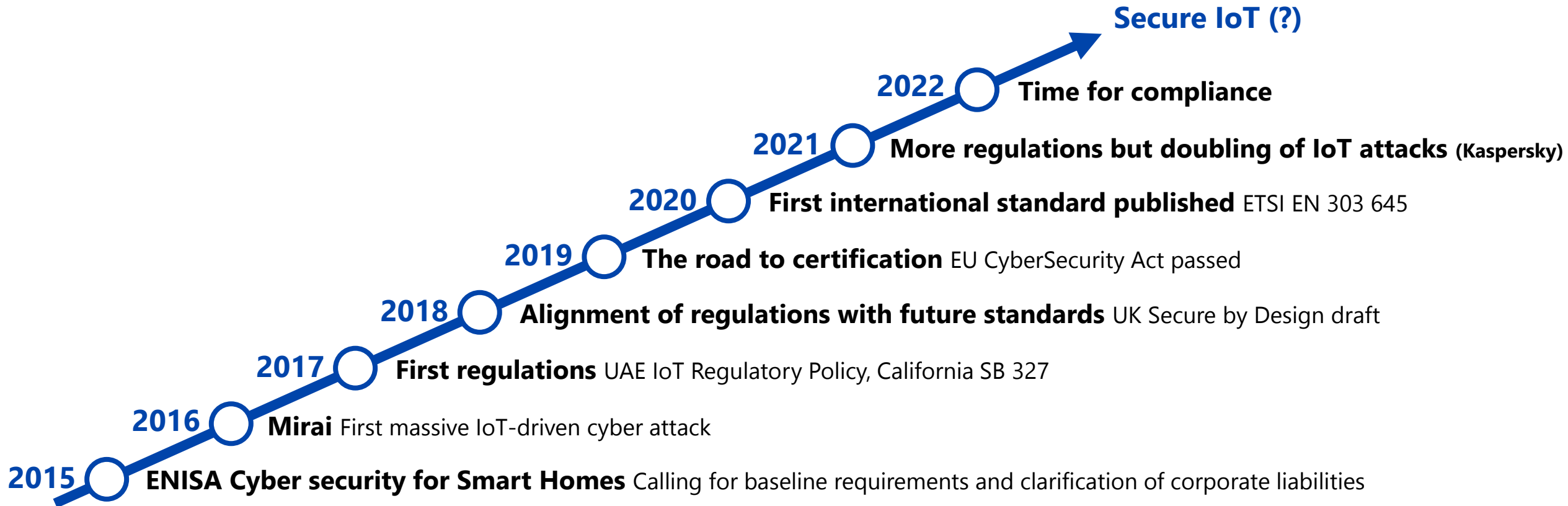
WHY IS REGULATION UNAVOIDABLE?

#IoTRegulations
#RegulateVendors



WHY IS REGULATION UNAVOIDABLE?

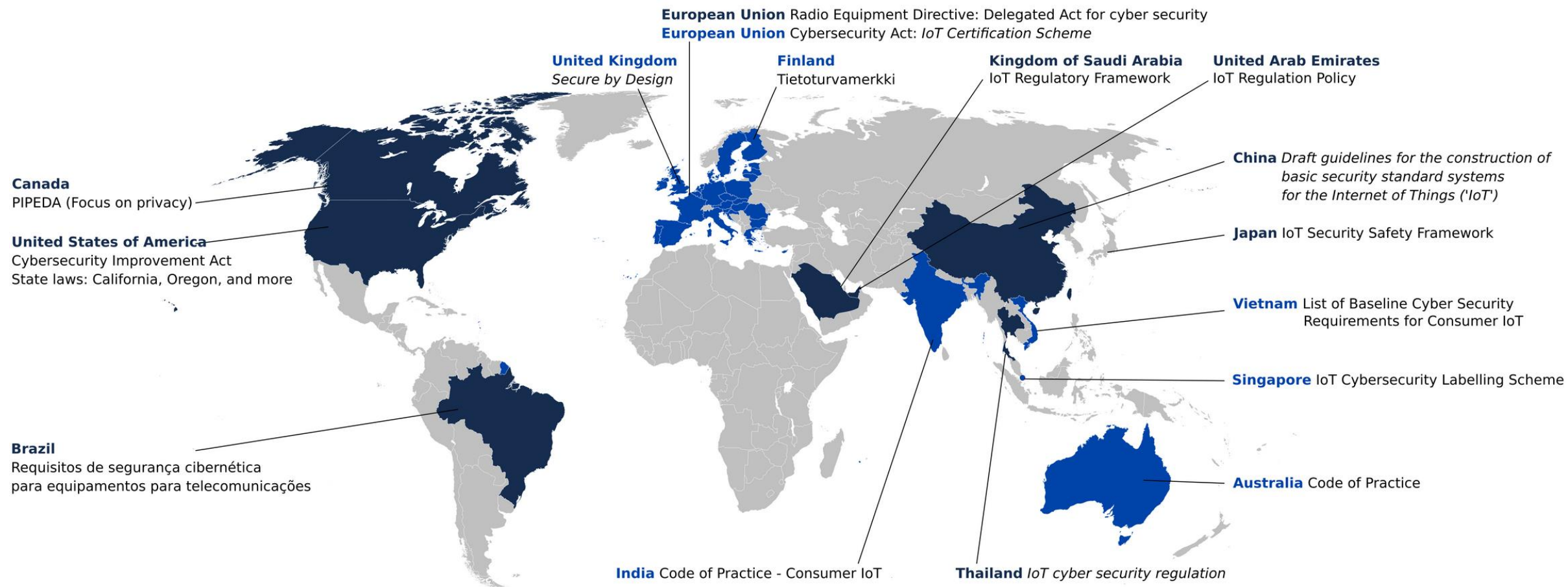
#IoTRegulations
#RegulateVendors



PANORAMA OF IoT CYBER SECURITY REGULATIONS #IoT Panorama

cetome.com/panorama

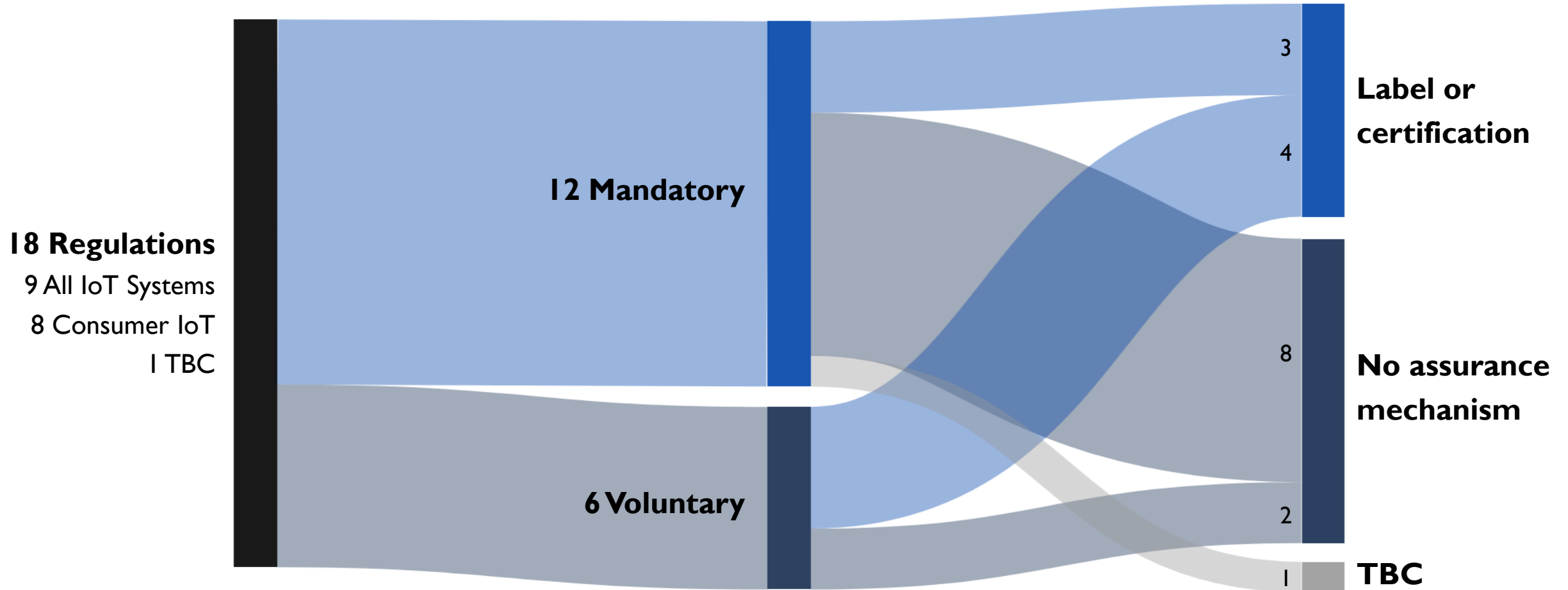
#IoT Regulations



■ Regulation based on ETSI EN 303 645
■ Possible compliance by following ETSI EN 303 645
On-going work

OVERVIEW OF IoT CYBER SECURITY REGULATIONS

#IoT Panorama
#IoT Regulations



DO YOUR OWN RESEARCH THEY SAY. HERE ARE THE RESULTS

#IoT Panorama

#IoT Regulations

Ensure regulation is fit for purpose

Baseline requirements (17/18)

Alignment with standards (all)

#RegulateVendors (17/18)

#RegulateEndUsers (2/18)

Some will #RegulateRetailers (2/18) and
#RegulateServiceProviders (3/18)

Ensure regulation is followed

Enforcement is key (12/18)

Assurance mechanisms to inform customers,
especially for voluntary regulations (4/6)

Self-assessment vs third-party certification



HOW TO SUCCEED IN A WORLD OF IoT REGULATIONS?

HOW TO SUCCEED IN A WORLD OF IoT REGULATIONS?

Policy Makers

Future-proof your policy requirements

Have **clear requirements** that do not leave place to interpretation

Rely on **international standards** for implementation and verification

Support regulated entities to achieve compliance

Have the means for **strong and fast enforcement**

Manufacturers and Regulated Entities

Have a **security governance for IoT** to drive compliance

Have **technical means** to meet baseline requirements

Must do:

- **Training** on requirements and standards
- **Threat modelling** and **risk assessment**
- Secure **implementation and verification**
- **Post-release security activities** (vulnerability management, secure patching)
- **Documentation** (in-house and for end users)

IoT SECURITY PROTIPS

Learn about ETSI EN 303 645 to achieve compliance with new regulations



**One Standard to
Rule IoT Security:
EN 303 645**

IoT Security Collection

Duration: ½ day

Audience: Project managers, programme managers, future IoT security experts, software developers, non-IoT security consultants, senior management

Objectives: **discover ETSI EN 303 645** and understand how you can **drive IoT cyber security in projects**



**Successfully
Implement
ETSI EN 303 645**

IoT Security Collection

Duration: 2 days

Audience: Software developers, product managers, IoT manufacturers, security consultants, security experts, auditors

Objectives: become proficient at ETSI EN 303 645 to **comply with IoT security regulations and achieve certification worldwide**

IoT SECURITY PROTIPS

Simplify threat modelling and compliance with #FAST (fast.cetome.com)

FAST >>>>
a Cetome project

[FAST Tool](#) [About FAST](#) [Contact Us](#)

FAST is your Friendly Assessment of Security and Threats

FAST is a methodology to simplify the lives of developers and product manufacturers. We designed FAST to inform the decision-process and speed up the adoption of security-by-design. FAST relies on a simple survey to perform an automatic threat modeling and elaborate a list of security measures adapted to your use-case. This proof-of-concept focuses on IoT security. Give it a try, it's free and we don't retain any data.

IoT Product Description

For each of the questions below, please pick one answer. If your product has a multiple usages, please choose the last answer.

1 Who will use the IoT product? *

Individual users (wearable, smart home)

A limited group of users (smart building, enterprise)

A large group of unrelated users (smart city, train station)

2 Where will this IoT product be installed? *

Wearable device

Indoors

Outdoors

3 Development process

Is the development process externalized to a third-party?
For example: white-label device, external development team.

Yes

Does the product use open source libraries?
Please select "Yes" if you don't know.

No

4 Who will install the product? *

The user

A trained person (installer, technician, engineer)

5 How long is the support period planned for? *

Note: this usually goes until the end-of-life of the product

1 year

2 years

3-5 years

> 5 years

IoT SECURITY PROTIPS

Simplify threat modelling and compliance with #FAST (fast.cetome.com)

71 Security Measures applicable

Do you need help for the next steps? Do you want to customize FAST? [Contact us!](#) We will be happy to help you.

[Export to CSV](#)

id	IoT security measures	Descriptions	Threats mitigated	ETSI provisions fulfilled	Decision	Top threats (occurrence)
[IoT-001]	Require password change at first boot	The easiest way to implement Security-by-Default.	[T-002] Broken authentication	[5.1-1]	Todo	31 threats computed [T-017] Information Leakage (9) [T-033] Legal threat (9)
[IoT-002]	Implement password rules to avoid basic default passwords	The default password must not be guessable nor follow a pattern: <i>password, password1, manufacturer123, admin</i>	[T-033] Legal threat [T-046] Backdoor	[5.1-1]	Counter-measure	[T-021] Issue related to security requirements (8) [T-008] Insecure dependency (8)
[IoT-003]	Generate secure individual passwords for each device.	When each device or service has its own randomly generated password, it becomes virtually impossible to guess.	[T-001] Lack of unique identity [T-002] Broken authentication [T-003] Unauthorized access	[5.1-3]	Will not be done	[T-032] Lack of Privacy Considerations (8) [T-040] Denial of Service (8) [T-044] Insecure protocols (8) [T-003] Unauthorized access (7)
[IoT-004]	Do not use public information to generate passwords.	It is easy for an attacker to guess the password for all devices when using public information (e.g. MAC address, Serial Number)	[T-001] Lack of unique identity [T-019] Reverse engineering	[5.1-3]	N/A	[T-034] Malicious Code (7) [T-023] Remote Code Execution (6) [T-035] Use of asset in cyberattacks (6)
[IoT-007]	Remove passwords for authentication	When communicating with Cloud systems, it is preferable to use tokens to protect authentication information. When using mobile applications, it is possible to rely on biometrics to authenticate a human user.	[T-001] Lack of unique identity [T-019] Reverse engineering	[5.1-3]	Todo	[T-016] Insecure encryption (6) [T-046] Backdoor (6)
[IoT-008]	Authenticate machine-to-machine communications with certificates	Certificates can be generated in factory or at first boot.	No threat computed but mandatory requirement from the standard	[5.1-3]	Todo	[T-006] Escalation of privileges (6) [T-037] Physical tampering (5) [T-041] Network Outage (5)



DISCUSSION ON THE FUTURE AND CONCLUSIONS

THE FUTURE OF IoT REGULATIONS

#IoTSecurity

Verification, certifications, labels, more regulations, globalisation

#RegulateVendors

ETSI TS 103 701 V1.1.1 (2021-08)



CYBER:
Cyber Security for Consumer Internet of Things:
Conformance Assessment of Baseline Requirements



How a European Cyber Resilience Act will help protect Europe

Published on September 16, 2021

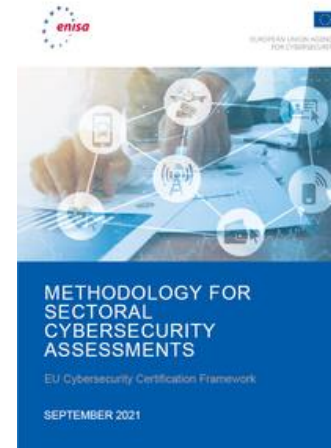
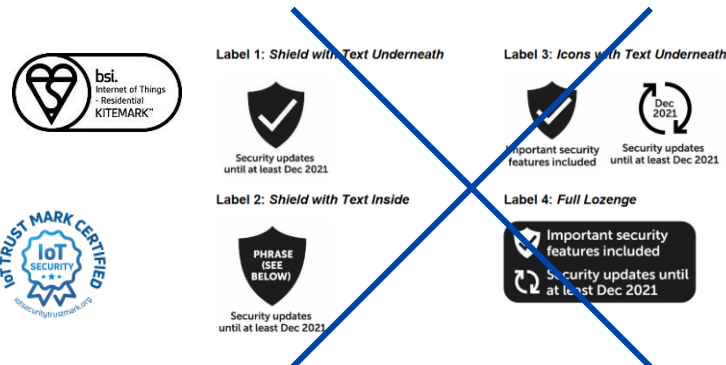
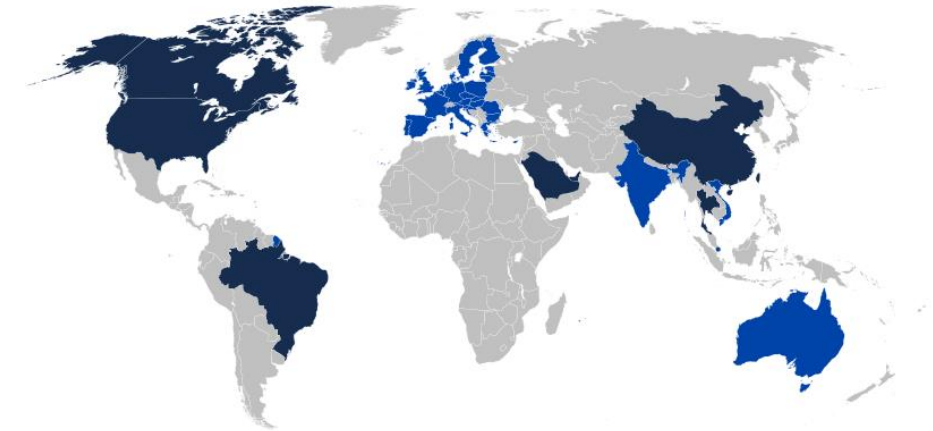


Thierry Breton

European commissioner for Internal market

95 articles

+ Follow



CONCLUSION

IoT Cyber Security Regulation is here

- Finally a way to secure IoT systems?
- Regulations must align with standards
- Support to manufacturers is key to success

Still a new domain

- Awareness remains an important topic
- Need for robust enforcement mechanisms
- Lack of harmonization globally

The “S” in IoT Security is a “R”

THANK YOU!

cetome.com