Packets & Policy

IoT Cyber Policy Landscape

Beau Woods

@beauwoods

I Am The Cavalry

@iamthecavalry

I Am The Cavalry

The Cavalry isn't coming... It falls to us

Problem Statement

Our society is adopting connected technology *faster than we are able to secure it*.

Mission Statement

To ensure connected technologies with the potential to impact public safety and human life are *worthy of our trust*.

Medical

Automotive

Connected Home

Public Infrastructure

Why Trust, public safety, human life
How Education, outreach, research
Who Infosec research community
Who Passionate volunteers
What Long-term vision for cyber safety

Collecting existing research, researchers, and resources

Connecting researchers with industry, media, policy, and legal

Collaborating across a broad range of backgrounds, interests, and skillsets

Catalyzing positive action sooner than it would have happened on its own

I Am The Cavalry
@beauwoods @iamthecavalry

Agenda

IoT Security Foundation

Annual Conference
December 4, 2018

Where are we now?

Important recent policies

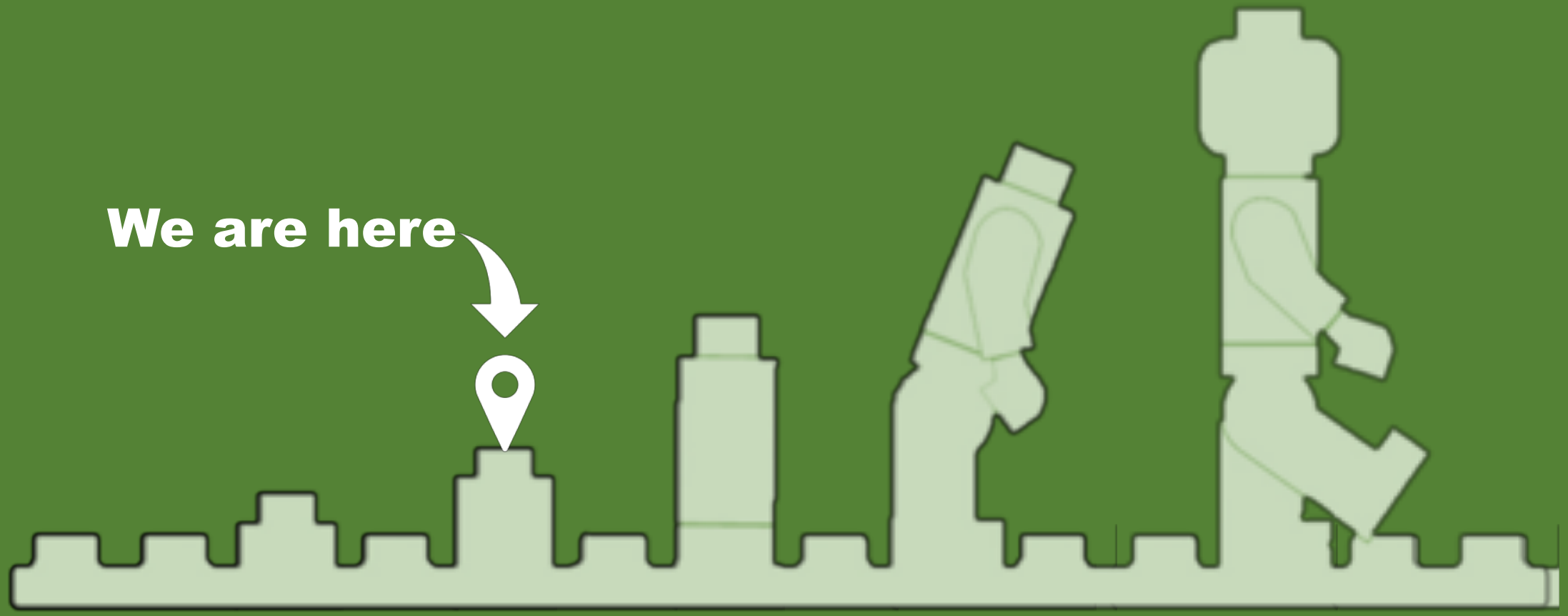
Where are we going?

- Tool: IoT Cyber Policy Database

Packets & Policy: IoT Cyber Policy Landscape

I Am The Cavalry
@beauwoods @iamthecavalry

Knowledge Evolves



Great London Fire, 1666

I Am The Cavalry
@beauwoods @iamthecavalry

Great London Fire, 1666

After 350 years of improvement, building fires are rare, stay contained, and are quickly extinguished.

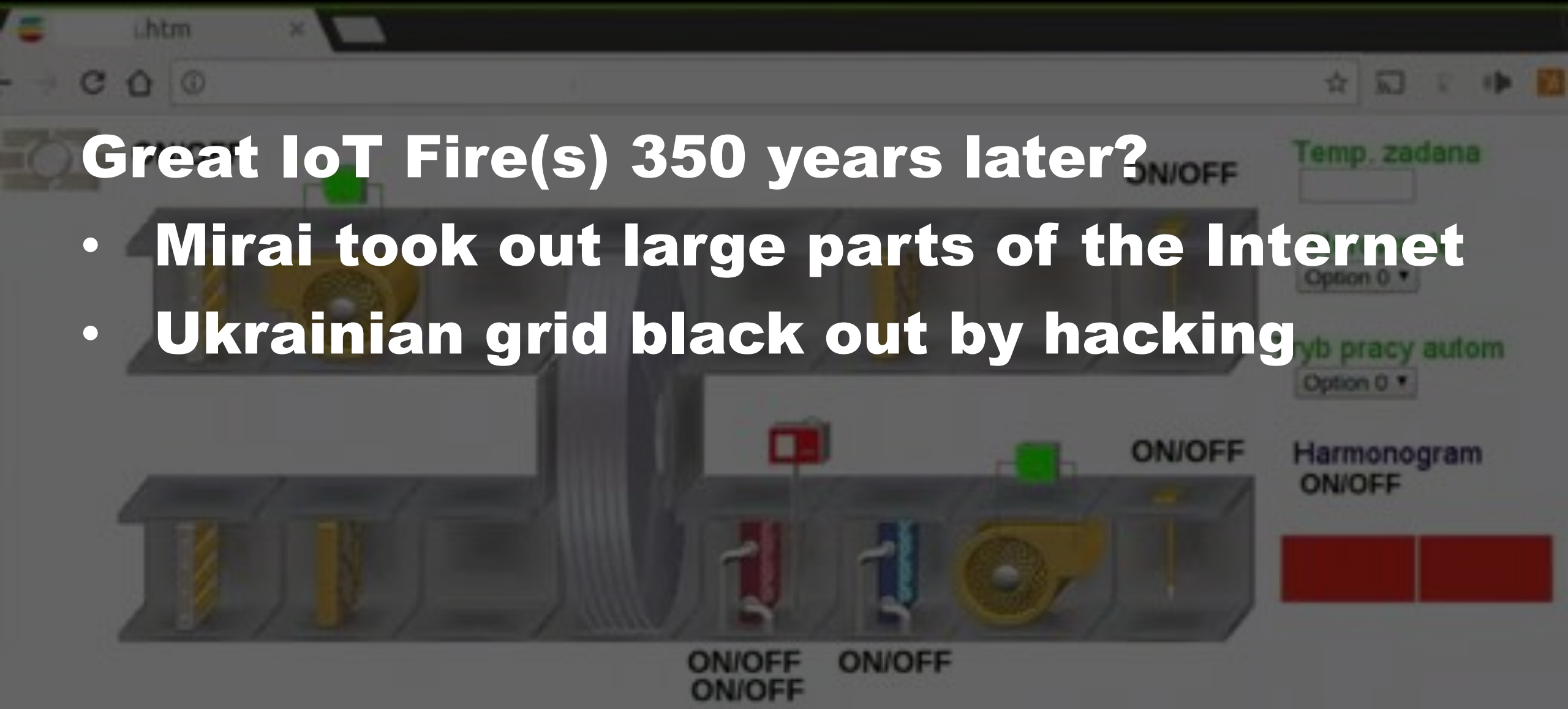
Great IoT Fire(s) 350 years later?

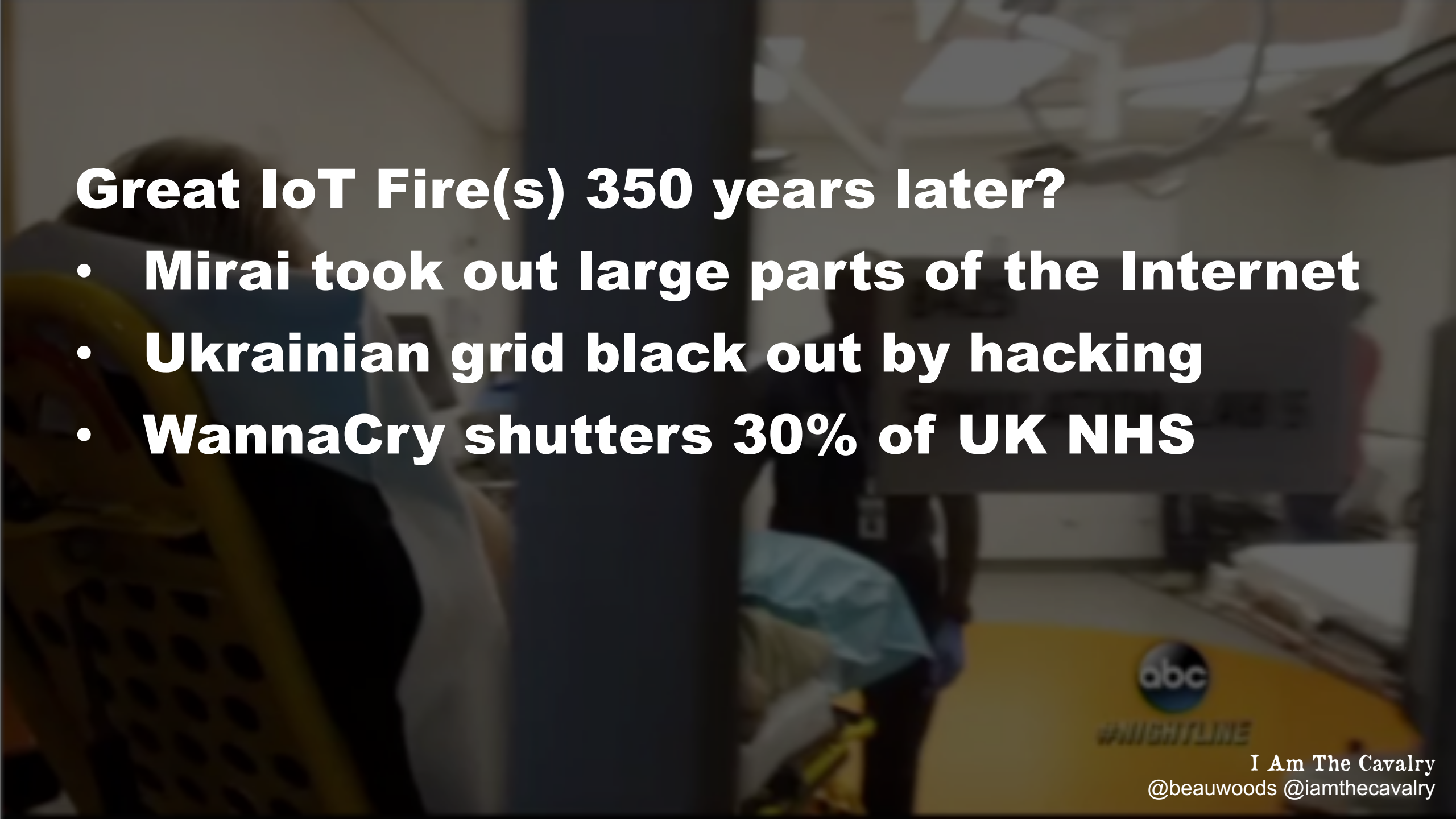
- Mirai took out large parts of the Internet

https://intel.malwaretech.com/pewpew.html

Great IoT Fire(s) 350 years later?

- Mirai took out large parts of the Internet
- Ukrainian grid black out by hacking





Great IoT Fire(s) 350 years later?

- Mirai took out large parts of the Internet
- Ukrainian grid black out by hacking
- WannaCry shutters 30% of UK NHS

I Am The Cavalry
@beauwoods @iamthecavalry

Great IoT Fire(s) 350 years later?

- Mirai took out large parts of the Internet
- Ukrainian grid black out by hacking
- WannaCry shutters 30% of UK NHS
- NotPetya disrupts global logistics & manufacturing, including vaccines

Public policy responses

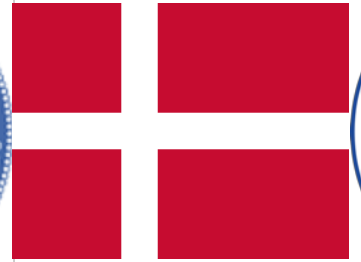
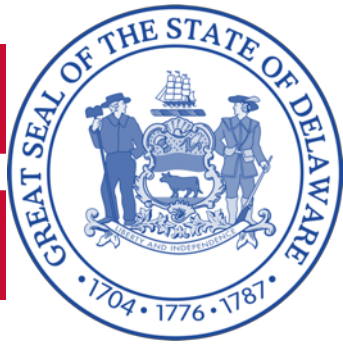
Europe
- EU
- ENISA
- UK DCMS
- BSI (DE)
- Denmark
- Netherlands

United States
- White House
- Military and Civilian Agencies
- Congress
- States

Private Sector, Academia
- “Charter of Trust”
- GSMA
- CTIA

I Am The Cavalry
@beauwoods @iamthecavalry



Important Recent Policies

Software Component Transparency

Code of Practice

SB 327

IoT Cyber Security Improvement Act

Premarket Guidance on Cybersecurity

I Am The Cavalry
@beauwoods @iamthecavalry

Department for Culture Media & Sport

GOV.UK

Code of Practice for IoT Security

https://www.gov.uk/government/publications/secure-by-design

Software Component Transparency

https://www.ntia.doc.gov/SoftwareTransparency

Software Component Transparency
Software Bill of Materials

SBOMs are already in use by several organizations, particularly in healthcare, while FDA is looking at how to increase usage.

https://www.ntia.doc.gov/SoftwareTransparency

Senate Bill 327
Signed Sep 28, 2018
Takes effect Jan 1, 2020

Similar to other privacy and security legislation already in effect in California

Requires manufacturers provide ***reasonable and appropriate*** security for IoT device design

Recommends (not mandates):

- No hardcoded default passwords
- Force password change on first use

As goes California, so goes the US, in public safety

What is ***reasonable and appropriate***?

Left to the IoT vendor to decide.

Draft Premarket Guidance for Cybersecurity in Medical Devices

- Based on real-world cases and lessons learned
- Capabilities and objectives, rather than controls

1. Authentication and authorization (people and code)
2. Code, data, and execution integrity
3. Evidence capture to support analysis and response
4. Fail safely and visibly
5. Transparency in cyber safety design and assumptions
6. Software component transparency (CBOM)
7. Cyber safety risk transparency

https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM623529.pdf

S.1691 - Internet of Things (IoT) Cybersecurity Improvement Act of 2017

115th Congress (2017-2018) | Get alerts

BILL Hide Overview ✖

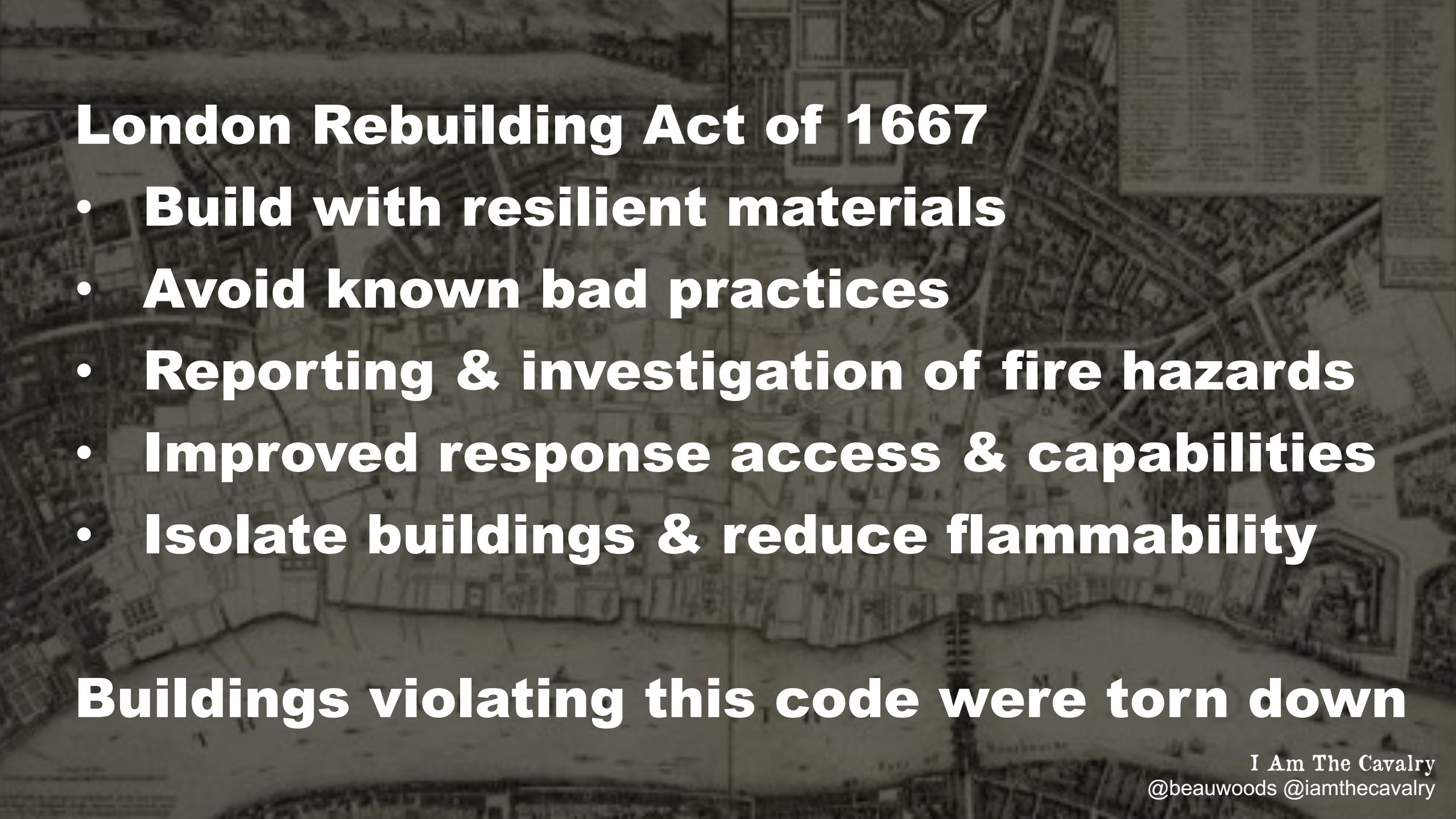
Anything sold to the US Government must:

A. Disclose known vulnerabilities
B. Be software updateable
C. Avoid hard-coded credentials
D. Have a coordinated disclosure policy

Where are we going?

We want to go this way

We are here



London Rebuilding Act of 1667

- Build with resilient materials
- Avoid known bad practices
- Reporting & investigation of fire hazards
- Improved response access & capabilities
- Isolate buildings & reduce flammability

Buildings violating this code were torn down

IoT cyber policy responses

- Build with resilient components
- Avoid known bad practices
- Coordinated vulnerability disclosure
- Prompt and secure software updates
- Isolate systems & reduce attack surface

Market/buyer empowerment and regulation

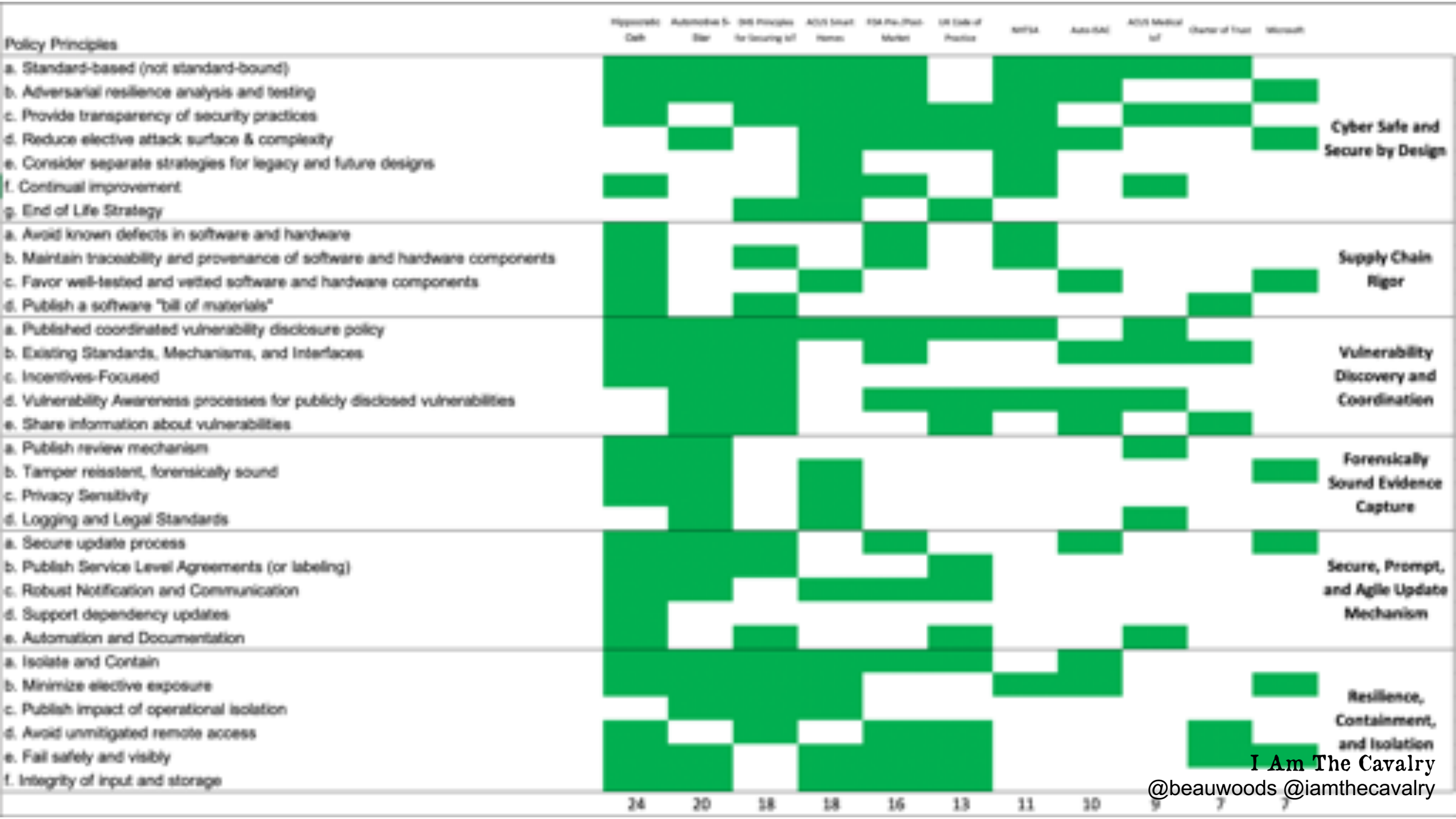
IoT Cyber Policy Database

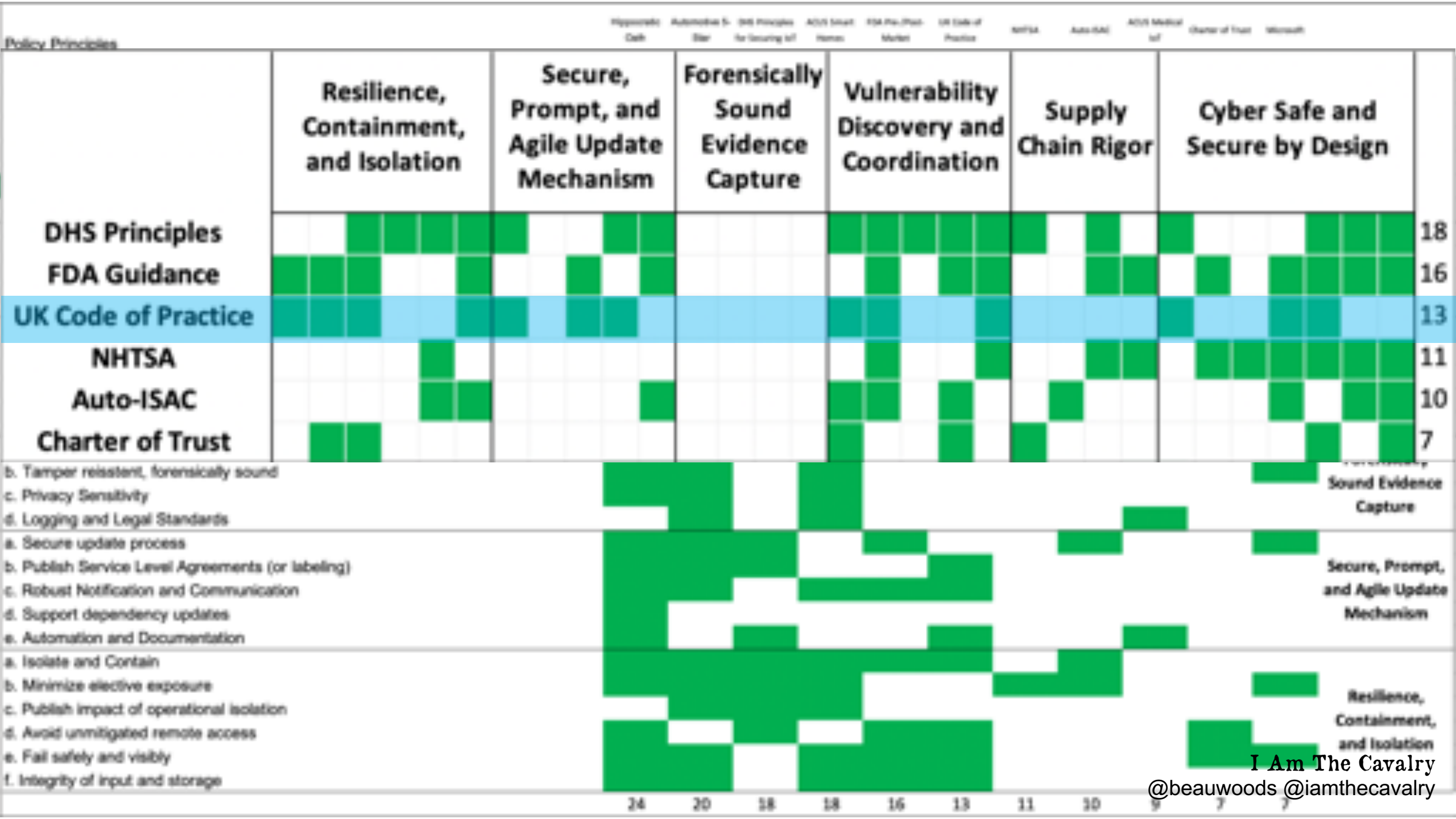
IoT Security Foundation

Annual Conference
December 4, 2018

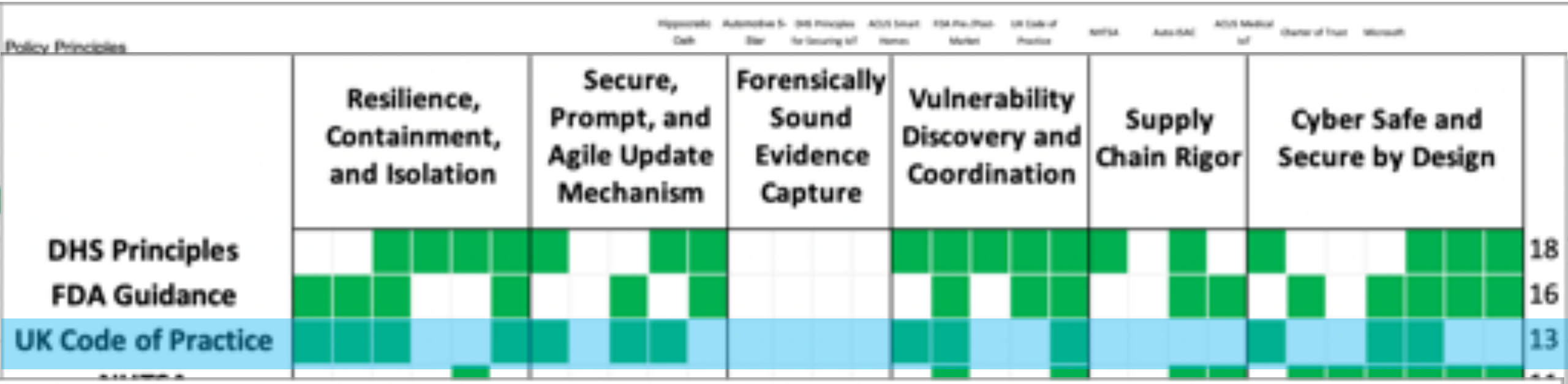
Packets & Policy: IoT Cyber Policy Landscape

I Am The Cavalry
@beauwoods @iamthecavalry


Policy Principles
Hippocratic Oath
Automotive S- Star
SHI Principles for Securing IoT
ACUS Smart Homes
FDA Pre-(Post-Market
UK Code of Practice
NHTSA
Auto-ISAC
ACUS Medical IoT
Charter of Trust
Microsoft
a. Standard-based (not standard-bound)
b. Adversarial resilience analysis and testing
c. Provide transparency of security practices
d. Reduce elective attack surface & complexity
e. Consider separate strategies for legacy and future designs
f. Continual improvement
g. End of Life Strategy
Cyber Safe and Secure by Design
a. Avoid known defects in software and hardware
b. Maintain traceability and provenance of software and hardware components
c. Favor well-tested and vetted software and hardware components
d. Publish a software "bill of materials"
Supply Chain Rigor
a. Published coordinated vulnerability disclosure policy
b. Existing Standards, Mechanisms, and Interfaces
c. Incentives-Focused
d. Vulnerability Awareness processes for publicly disclosed vulnerabilities
e. Share information about vulnerabilities
Vulnerability Discovery and Coordination
a. Publish review mechanism
b. Tamper reisstent, forensically sound
c. Privacy Sensitivity
d. Logging and Legal Standards
Forensically Sound Evidence Capture
a. Secure update process
b. Publish Service Level Agreements (or labeling)
c. Robust Notification and Communication
d. Support dependency updates
e. Automation and Documentation
Secure, Prompt, and Agile Update Mechanism
a. Isolate and Contain
b. Minimize elective exposure
c. Publish impact of operational isolation
d. Avoid unmitigated remote access
e. Fail safely and visibly
f. Integrity of input and storage
Resilience, Containment, and Isolation
24
20
18
18
16
13
11
10
9
7
7
I Am The Cavalry
@beauwoods @iamthecavalry



I Am The Cavalry
@beauwoods @iamthecavalry



Resilience, Containment, and Isolation

- **Minimize elective exposure.** Connectivity can provide critical capabilities. It also increases exposure to hazardous conditions and adversaries. Exposure that does not meaningfully improve capabilities adds attack surface. As such, more secure and lower (total) cost designs seek to minimize these types of exposure.
- **Avoid unmitigated remote access.** Capabilities in the hands of an operator, working in good faith, can be used for harm in the hands of an adversary or unskilled individual. Credentials gating remote access must remain unknown to adversaries yet available to defenders. Hard coded or default credentials (passwords, keys, etc.), absent other gating methods, cannot assure security or safety, so should be avoided or augmented.

To be publicly released soon.
Email info [at] iamthecavalry.org
for prerelease version

Resilience, Containment, and Isolation

- **Minimize elective exposure.** Connectivity can provide critical capabilities. It also increases exposure to hazardous conditions. Connectivity exposure that does not meaningfully improve capabilities adds attack surface. As such, more secure and lower (total) cost designs seek to minimize these types of exposure.
- **Avoid unmitigated remote access.** Capabilities in the hands of an operator, working in good faith, can be used for harm in the hands of an adversary or unskilled individual. Credentials gating remote access must remain unknown to adversaries yet available to defenders. Hard coded or default credentials (passwords, keys, etc.), absent other gating methods, cannot assure security or safety, so should be avoided or augmented.

Packets & Policy

IoT Cyber Policy Landscape

Beau Woods

@beauwoods

I Am The Cavalry

@iamthecavalry