The Standards People

IoT Conference 2023

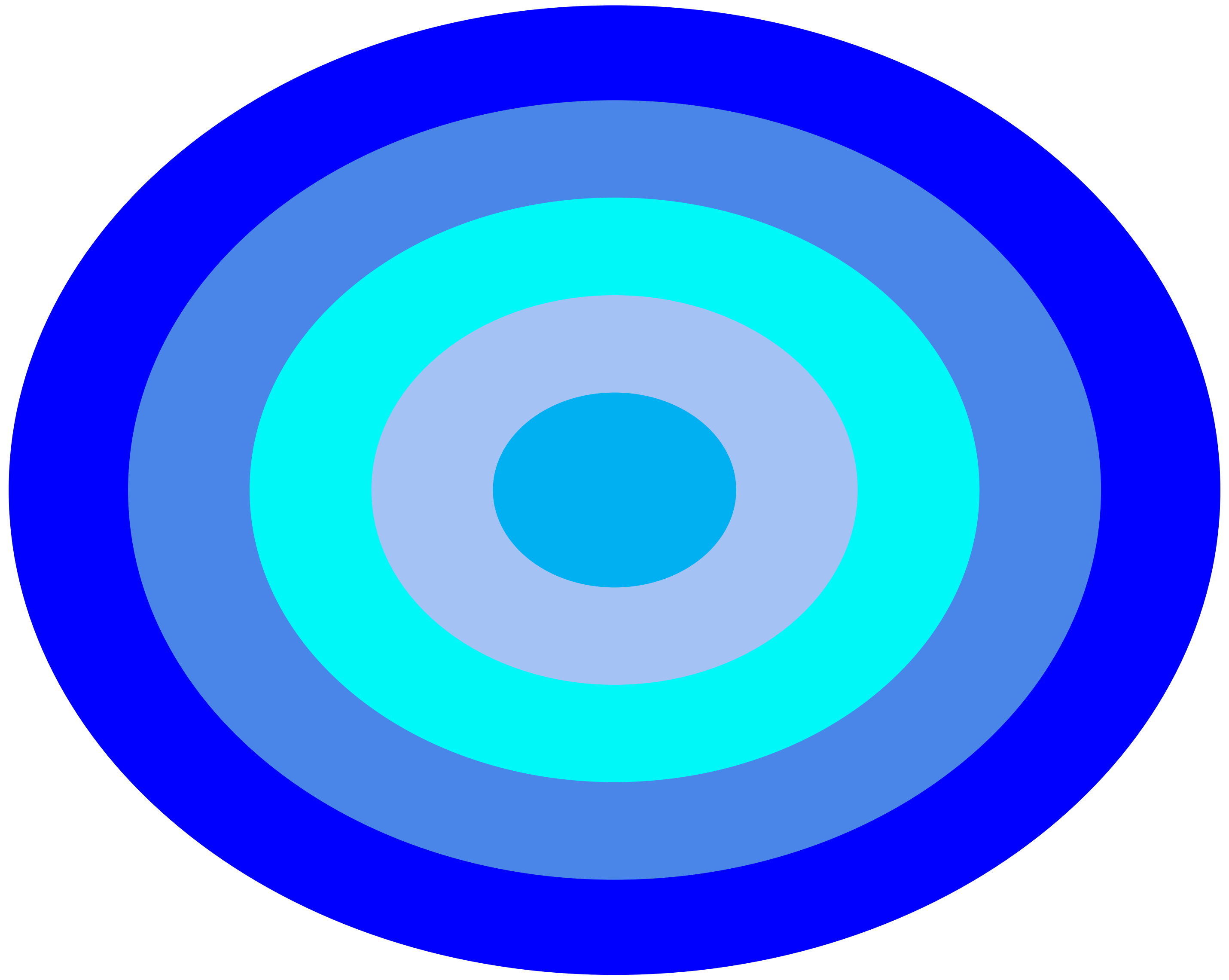
Introduction to DSIT Policy for Enterprise IoT and the potential for international standards

Presented by:

Department for
Science, Innovation
& Technology

James Deacon & Rhys Duncan

Department for
Science, Innovation
& Technology



Core Objective

Protect users, networks and infrastructure from vulnerable connected products (IoT)

IoT Product Security - our work to date

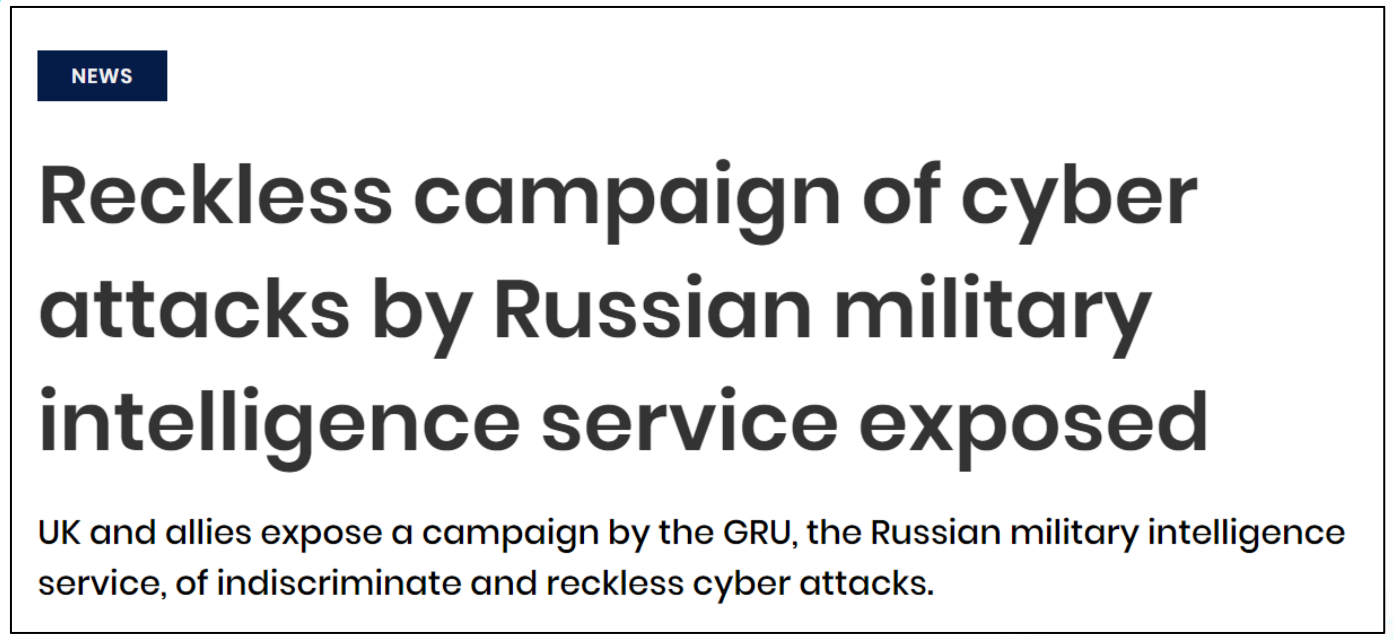
Consumer IoT

Enterprise IoT

Industrial IoT

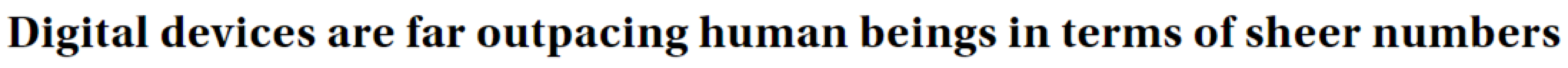
Department for Science, Innovation & Technology

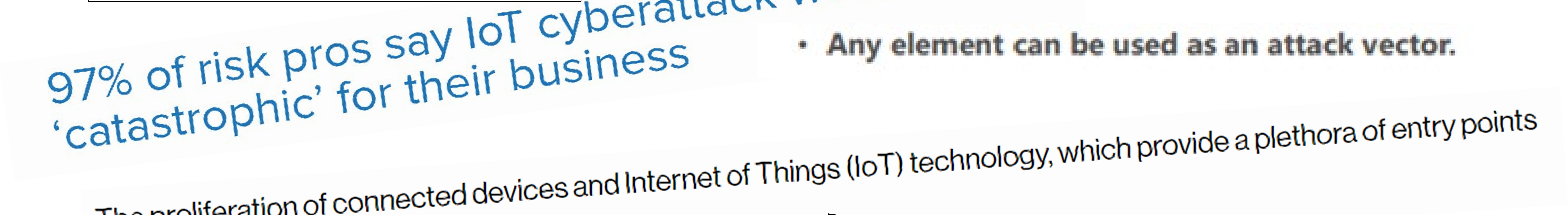
The problem


NEWS

Reckless campaign of cyber attacks by Russian military intelligence service exposed

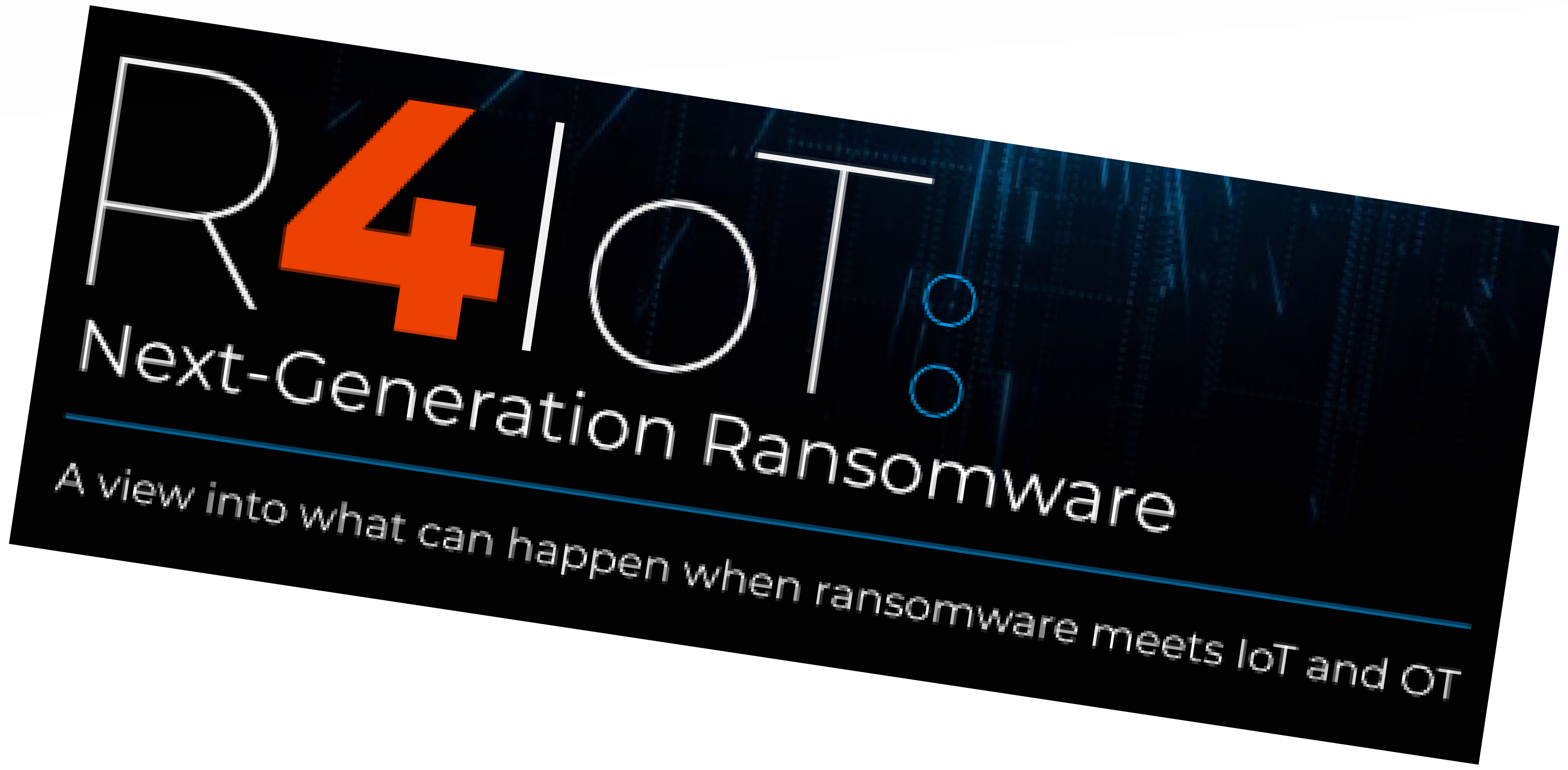
UK and allies expose a campaign by the GRU, the Russian military intelligence service, of indiscriminate and reckless cyber attacks.


Digital devices are far outpacing human beings in terms of sheer numbers


97% of risk pros say IoT cyberattack would be 'catastrophic' for their business

- Any element can be used as an attack vector.

The proliferation of connected devices and Internet of Things (IoT) technology, which provide a plethora of entry points for cybercriminals;


R4IoT: Next-Generation Ransomware

A view into what can happen when ransomware meets IoT and OT

Enterprise's and their networks offer attackers:

- A broader attack surface
- Potentially higher value data
- Chance of greater scale of impact

Department for
Science, Innovation
& Technology

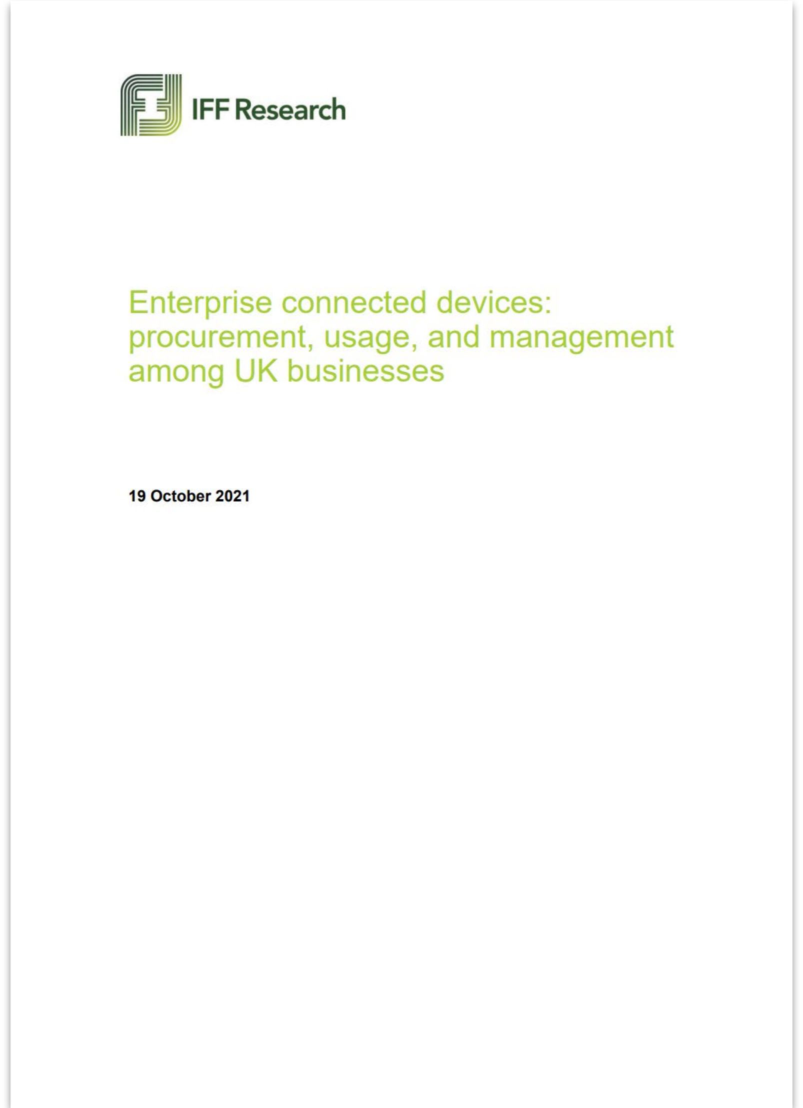
The scope

This includes:

- Enterprise printers
- Video conferencing systems
- VoIP phones
- Network Attached Storage (NAS) devices
- Room booking displays
- IP Camera
- Laptops
- Smartphones
- Connected devices used in an enterprise environment on a corporate network

Department for
Science, Innovation
& Technology

Our work to date

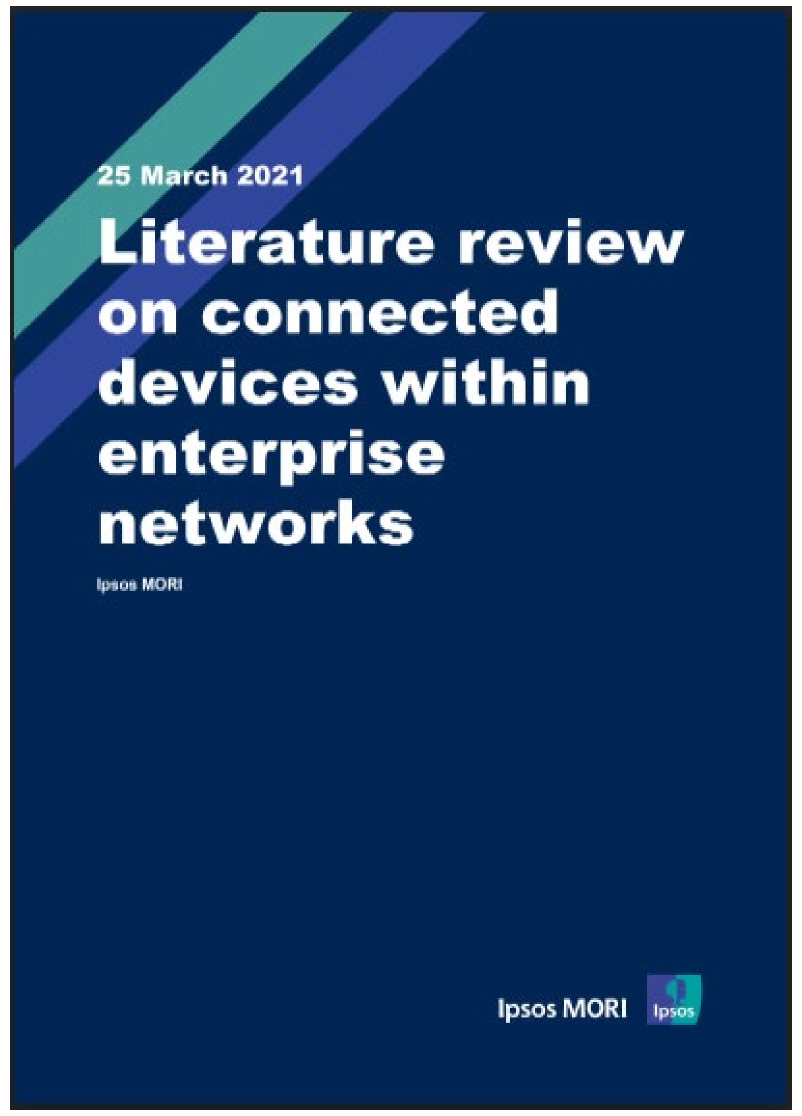


IFF Research

Enterprise connected devices: procurement, usage, and management among UK businesses

19 October 2021

Business Survey (2021)



25 March 2021

Literature review on connected devices within enterprise networks

Ipsos MORI

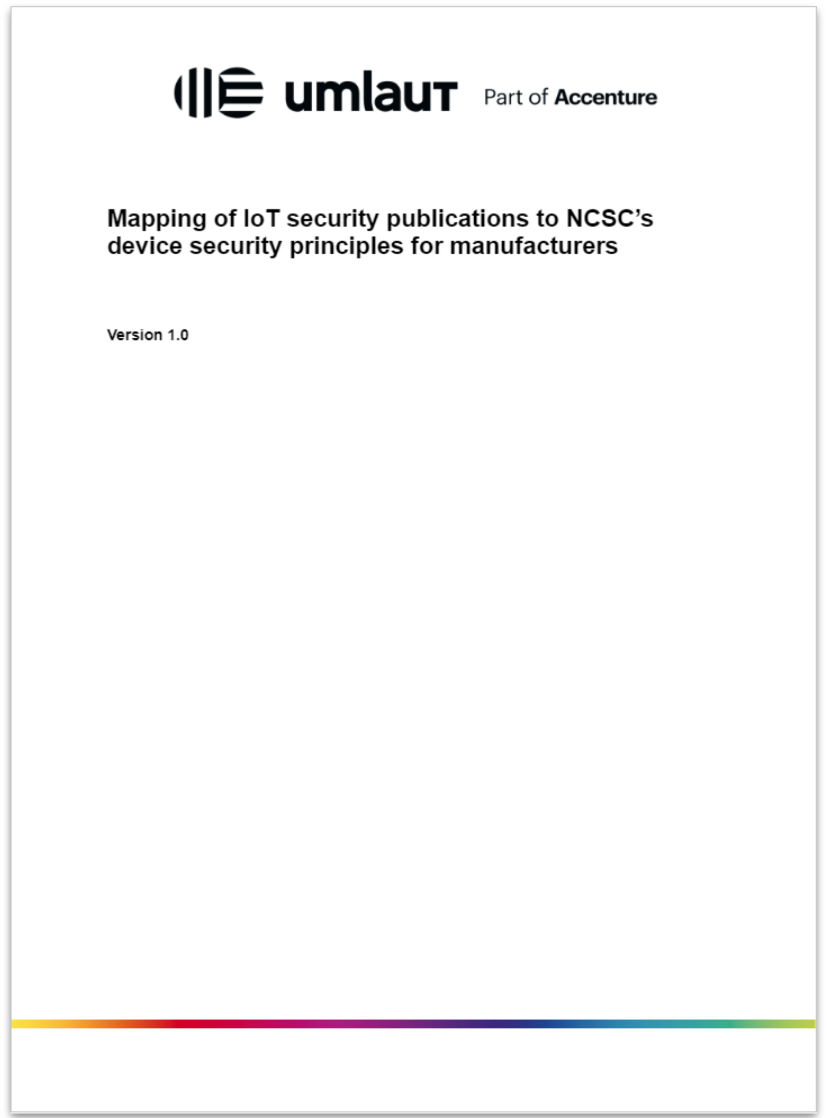
Ipsos MORI

Literature Review (2021)

National Cyber Security Centre
a part of GCHQ

The Threat to Enterprise use

NCSC-A Report (2021)

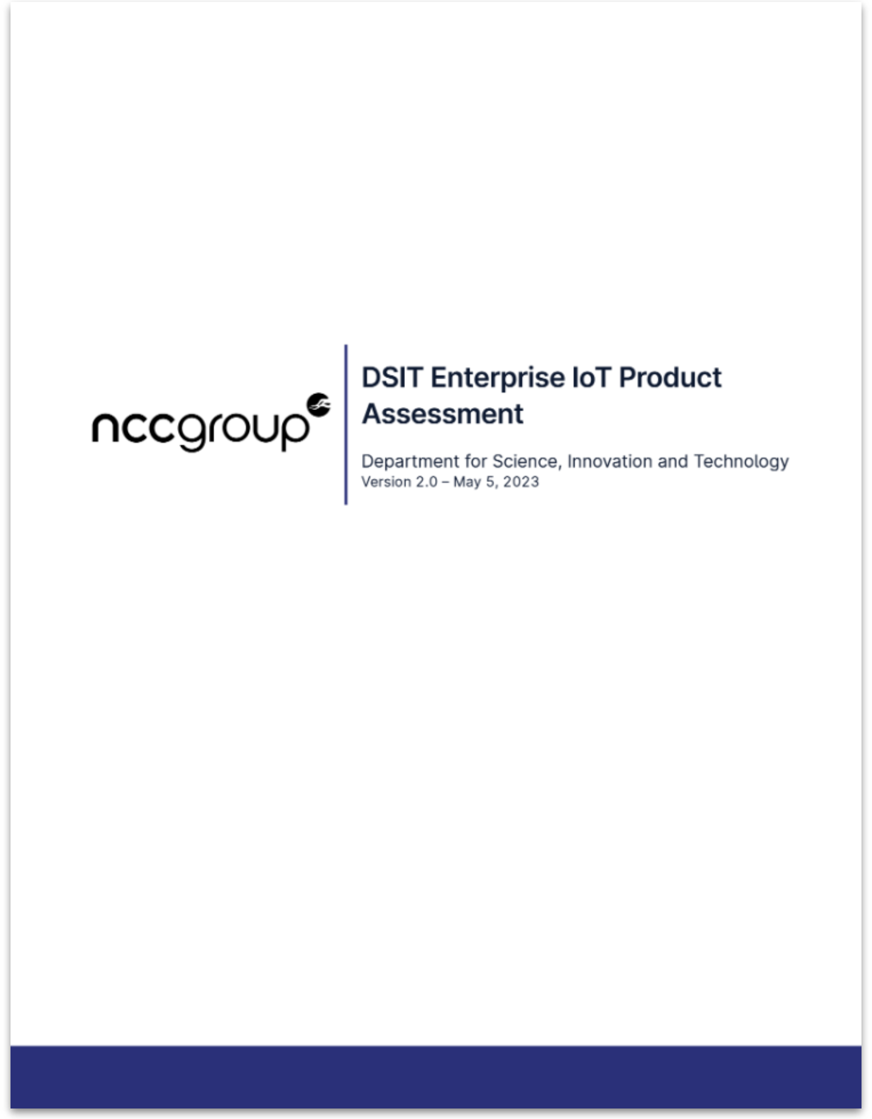


umlaut Part of Accenture

Mapping of IoT security publications to NCSC's device security principles for manufacturers

Version 1.0

Mapping of enterprise IoT security publications to NCSC's Device Security Principles (TBC 2023)



nccgroup

DSIT Enterprise IoT Product Assessment

Department for Science, Innovation and Technology
Version 2.0 – May 5, 2023

Product testing of enterprise IoT devices (TBC 2023)

Our findings

- Enterprise connected devices are being deployed and relied on by many organisations, however there are significant concerns from IT professionals about device security.
- Organisations lack clarity on how to monitor and protect themselves from devices
- Our mapping identified a number of areas where best practice could be more widely accepted by manufacturers to help protect users.
- Vulnerabilities are regularly found in enterprise connected devices which have put large numbers of organisations at risk.
- For example, our grant into the product testing of some common enterprise IoT devices found that:
  - Price does not guarantee better security
  - Lack of secure boot or integrity protection
  - Physical access compromise
  - Outdated software is being widely used
  - Lack of privilege separation
  - General insecure configuration

Department for
Science, Innovation
& Technology

Introducing NCSC's Device Security Principles for manufacturers - a basis for a new international standard?

1. Provide updates, securely
2. Support appropriate authentication
3. Protect data at rest and in transit
4. Maintain device integrity
5. Ensure transparency of device health
6. Permit only trusted software
7. Minimise the privilege and reach of applications
8. Constrain the use of all device interfaces
9. Allow robust device management
10. Provide security logging, alerting, and monitoring
11. Enable recovery to a known good state

- Principles are not ordered by importance, but adjacent ones are often related
- Each principle contains a set of guidelines
- Principles describe the overall objective
- A framework that helps us work with industry to drive forward security standards in Enterprise Connected Devices

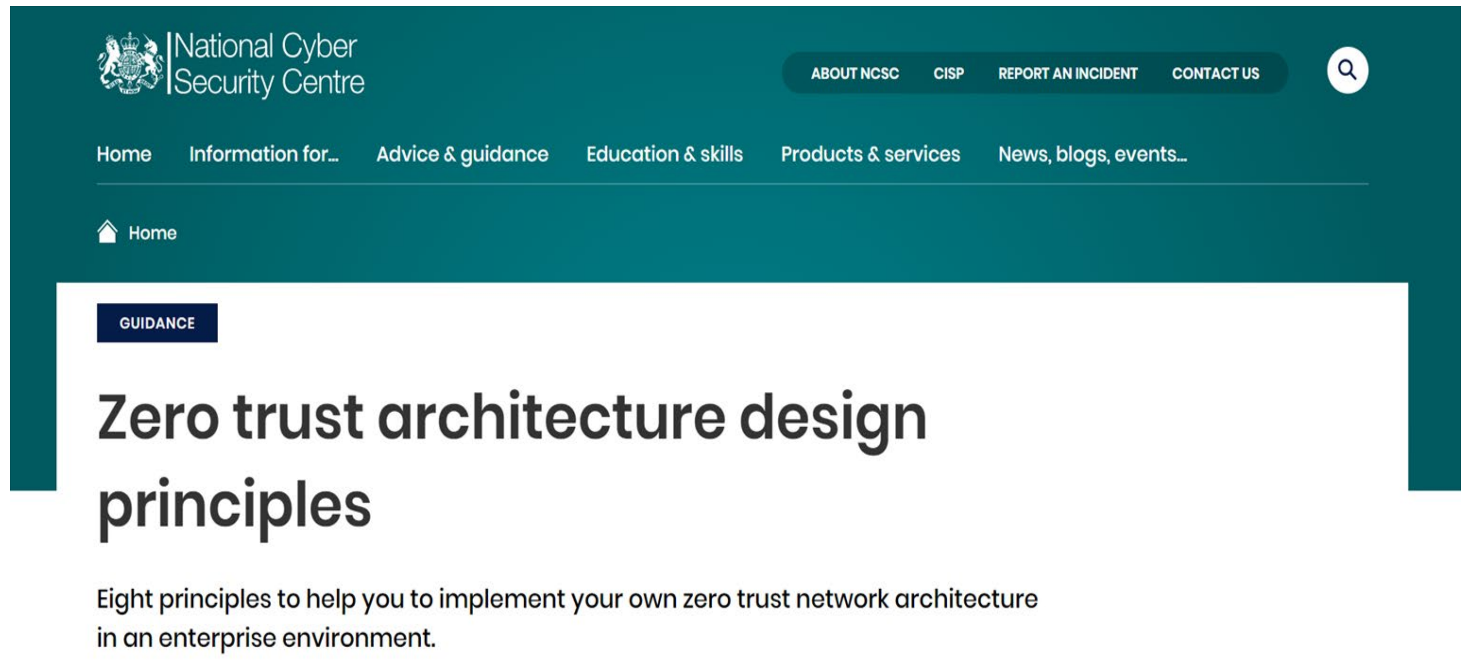
Department for
Science, Innovation
& Technology

The foundation of the principles

ETSI EN 303 645 V2.1.1 (2020-06)

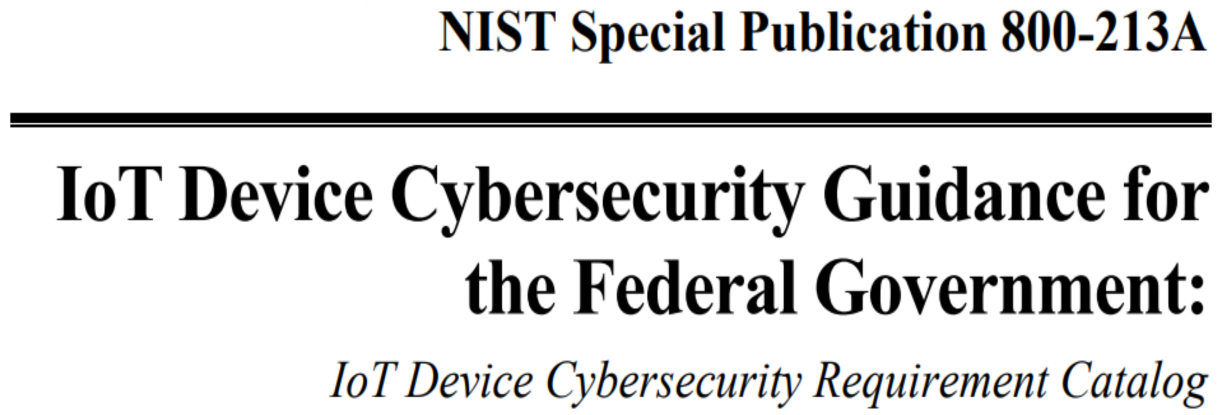
NISTIR 8259A

IoT Device Cybersecurity Capability Core Baseline



Zero trust architecture design principles

Eight principles to help you to implement your own zero trust network architecture in an enterprise environment.


NIST Special Publication 800-213A

IoT Device Cybersecurity Guidance for the Federal Government:

IoT Device Cybersecurity Requirement Catalog

MITRE | ATT&CK®

Principles & Guidelines that keep at its core:

- Recognition of the move away from the traditional network security perimeter
- Detecting compromise through device health
- The wide range of Enterprise Connected Devices

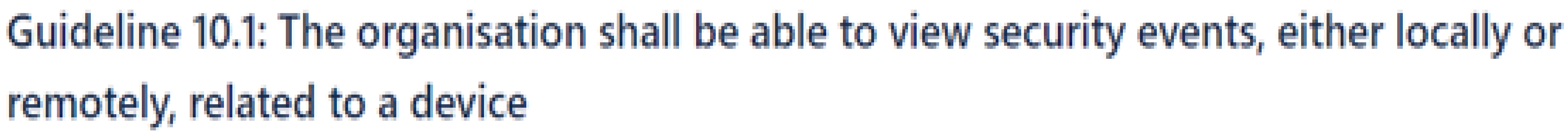
Principle 1: Provide updates, securely

- Guideline 1.1: The manufacturer shall publish the minimum period for which the device will receive security updates.
- Guideline 1.2: The device shall verify that an update is from a trusted source and that it wasn't altered during transit.
- Guideline 1.3: The device should use best-practice cryptography to support secure updates.
- Guideline 1.4: The manufacturer shall publish a policy defining the regularity and frequency of updates.
- Guideline 1.5: Device updates shall be provided in response to critical vulnerabilities and incidents.
- Guideline 1.6: Updates shall be manageable and flexible for administrators or other authorised entities (either users or other devices or services) across device fleets.
- Guideline 1.7: Details of updates shall be published that state which publicly known vulnerabilities have been mitigated.

ETSI EN 303 645

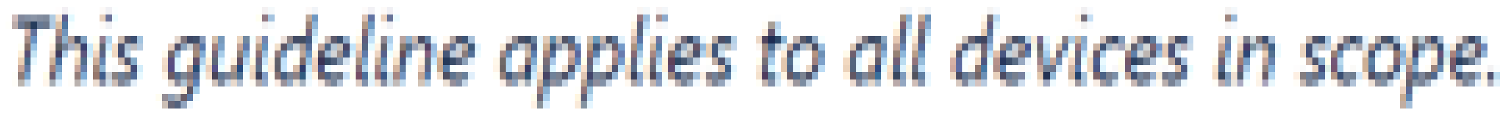
The structure

Guidelines explain how we expect a principle to be met:

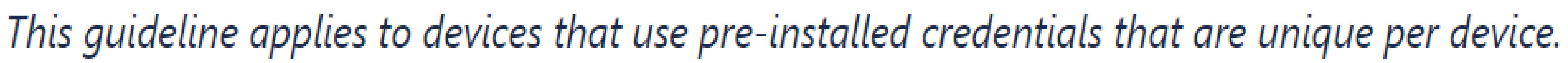


Guideline 10.1: The organisation shall be able to view security events, either locally or remotely, related to a device

Guidelines explain if they apply to only some device types in scope:

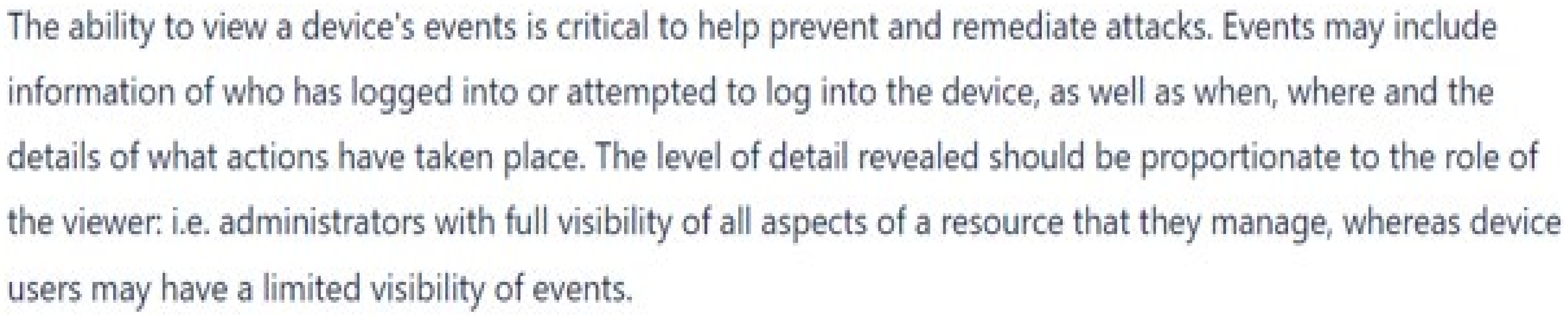


This guideline applies to all devices in scope.



This guideline applies to devices that use pre-installed credentials that are unique per device.

Guidelines describe the threats and risks that require mitigation:

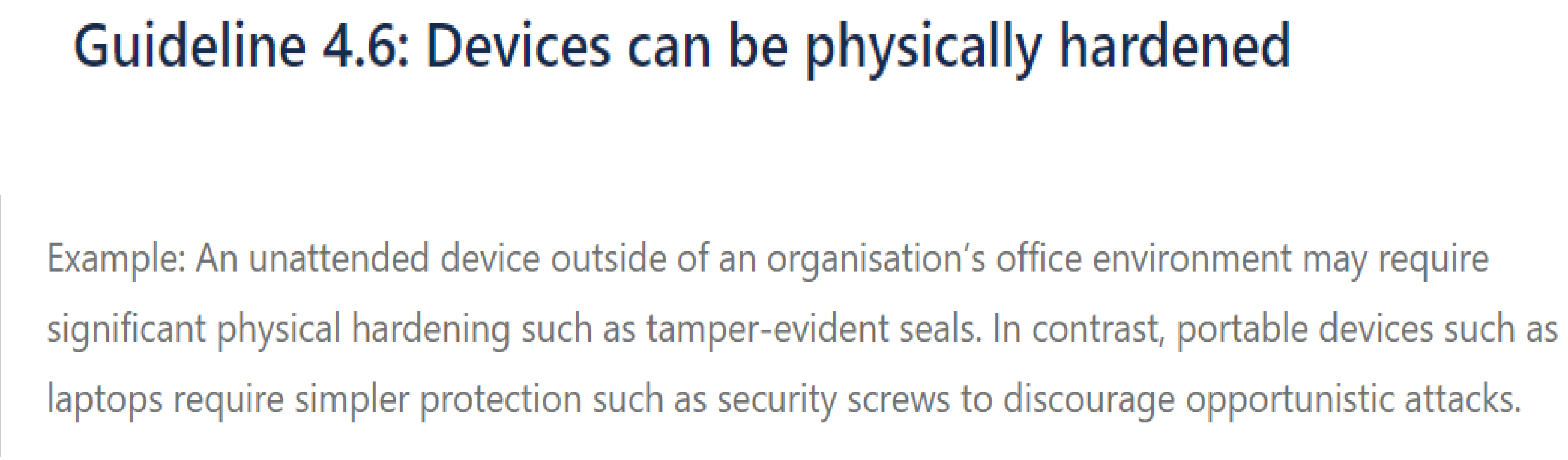


The ability to view a device's events is critical to help prevent and remediate attacks. Events may include information of who has logged into or attempted to log into the device, as well as when, where and the details of what actions have taken place. The level of detail revealed should be proportionate to the role of the viewer: i.e. administrators with full visibility of all aspects of a resource that they manage, whereas device users may have a limited visibility of events.

Department for
Science, Innovation
& Technology

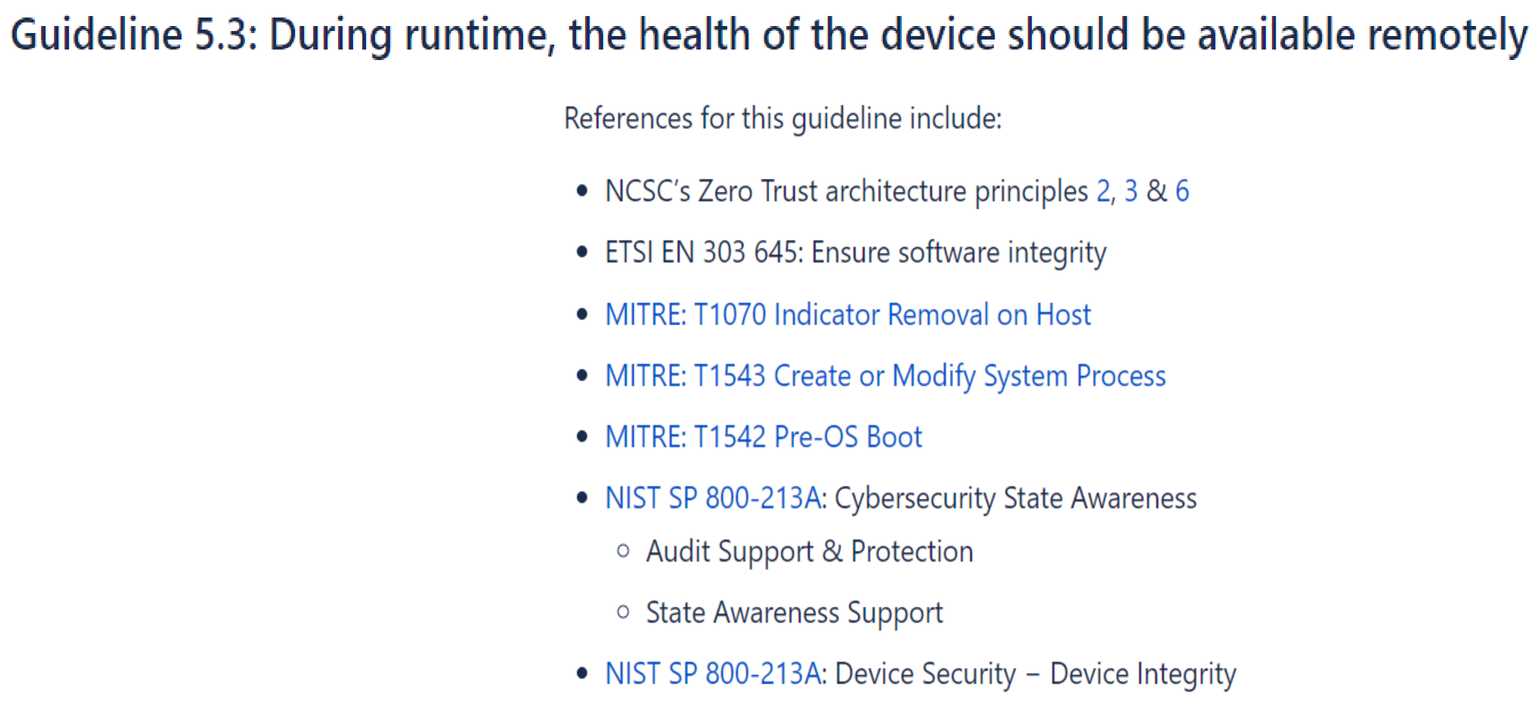
The structure (conǂd)

Guidelines include examples and references to provide clarity:



Guideline 4.6: Devices can be physically hardened

> Example: An unattended device outside of an organisation's office environment may require significant physical hardening such as tamper-evident seals. In contrast, portable devices such as laptops require simpler protection such as security screws to discourage opportunistic attacks.

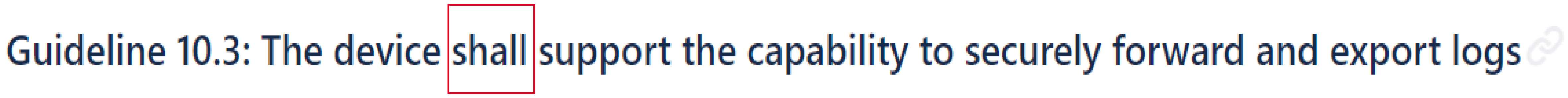


Guideline 5.3: During runtime, the health of the device should be available remotely

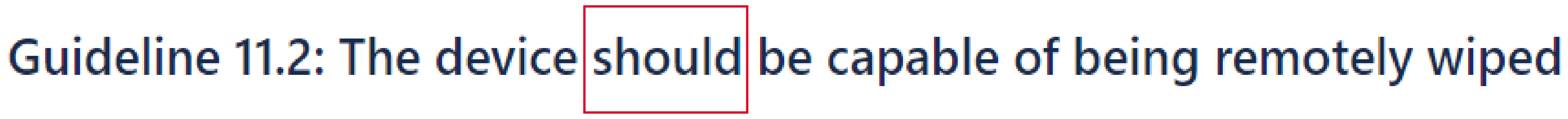
References for this guideline include:

- NCSC's Zero Trust architecture principles 2, 3 & 6
- ETSI EN 303 645: Ensure software integrity
- MITRE: T1070 Indicator Removal on Host
- MITRE: T1543 Create or Modify System Process
- MITRE: T1542 Pre-OS Boot
- NIST SP 800-213A: Cybersecurity State Awareness
  - Audit Support & Protection
  - State Awareness Support
- NIST SP 800-213A: Device Security – Device Integrity

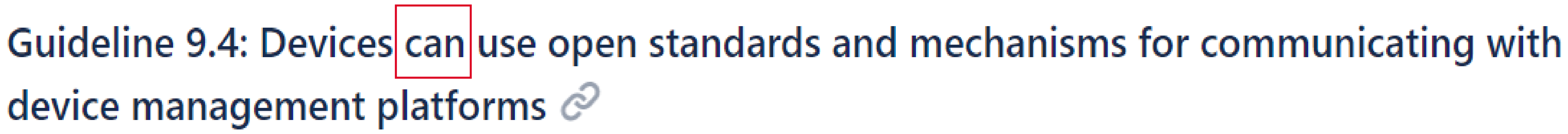
Guidelines use modal verbs in line with IETF RFC2119 and the ETSI Drafting Rules:



Guideline 10.3: The device shall support the capability to securely forward and export logs



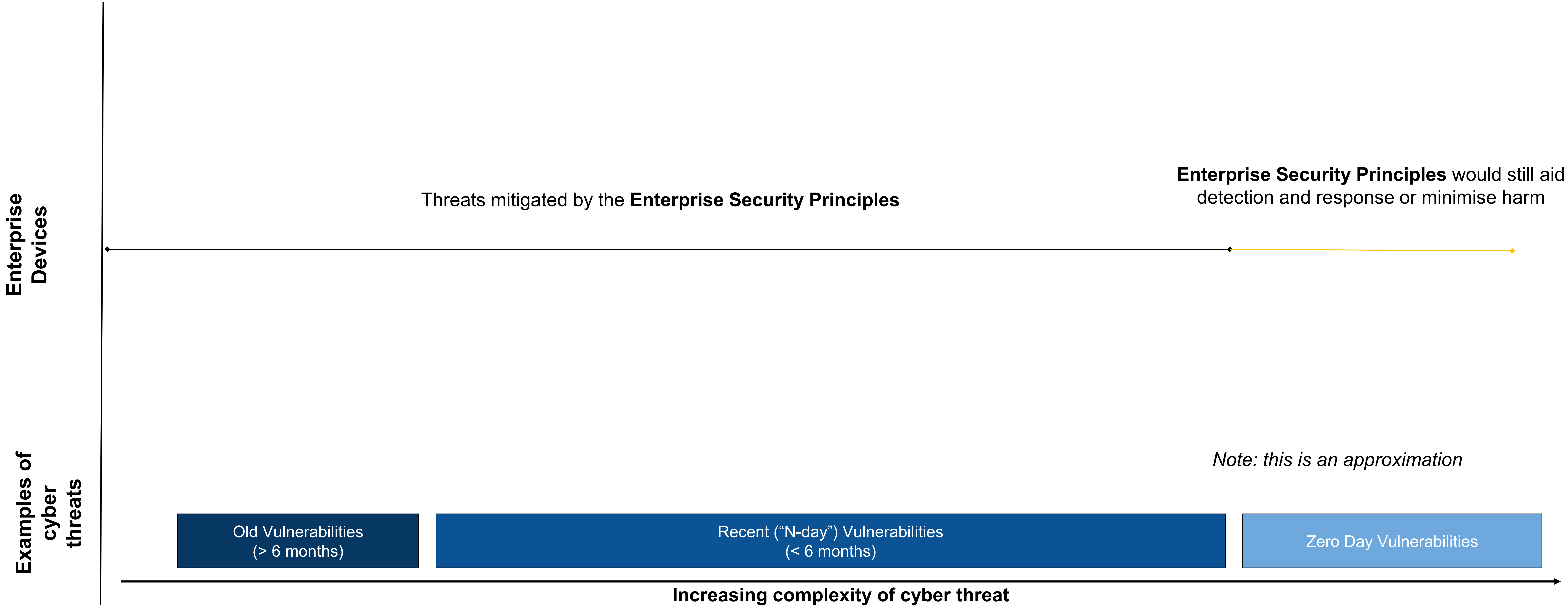
Guideline 11.2: The device should be capable of being remotely wiped



Guideline 9.4: Devices can use open standards and mechanisms for communicating with device management platforms

Department for
Science, Innovation
& Technology

Where does it fit?



Threats mitigated by the **Enterprise Security Principles**

Enterprise Security Principles would still aid detection and response or minimise harm

Note: this is an approximation

Enterprise Devices
Examples of cyber threats
Old Vulnerabilities (> 6 months)
Recent ("N-day") Vulnerabilities (< 6 months)
Zero Day Vulnerabilities
Increasing complexity of cyber threat

Principle 4: Maintain device integrity

- Guideline 4.1: The firmware and operating system on the device shall only be modifiable using authorised update mechanisms.

- Guideline 4.2: The device shall support pre-operating system boot security.

- Guideline 4.3: The device should have a built-in framework for runtime integrity protection.

- Guideline 4.4 The device shall provide documented exploit mitigation capabilities that shall be used by all system and pre-installed software.

- Guideline 4.5: Integrity of device health data should be maintained on the device.

- Guideline 4.6: The device can be physically hardened.

Our vision and next steps

- Consultation on our work, the current principles and future interventions

- One option: principles to be refined (for example, SBOMs?) and introduced as a new work item, e.g. in TC Cyber?

- Explore other levers to help organisations with their procurement, deployment and management of enterprise connected devices on their corporate networks

Department for
Science, Innovation
& Technology

James.Deacon@dcms.gov.uk
Rhys.Duncan@dcms.gov.uk
Matt.H5@ncsc.gov.uk