SOFTWARE UPDATES

Emily Taylor, Oxford Information Labs
Michael Richardson, Sandelman Software Works

IoT Security Foundation

OXFORD INFORMATION LABS

Course Aims

This course aims to :

- Introduce new guidance, EN 303 645, and upcoming regulation
- Give an overview of common update processes
- Explain the mechanics of updates and need for recovery
- Deal with design choice relating to updates

Learning outcomes

By the end of the course, you should understand:

- New requirements/regulations for updates
- What is required to make updates work smoothly
- How to plan for recovery from update failures
- How to find an update solution for your environment

Security and Technical Education Programme (STEP)

- IoT Security Foundation Quick Guides & training webinars
  - No universal default passwords
  - Managing coordinated vulnerability disclosure
  - Security software updates
- Industry and private sector-led
- Worked closely with UK government
- Technical and regulatory experts

IoT Security Foundation

OXFORD INFORMATION LABS

Who is this course aimed at?

SMEs, start-ups, innovators and researchers

Engage people across the organization…

- Product Manager
- Product Development Manager
- Supply Chain Manager
- Software Release Team
- Head of Design
- Product Security Team
- Compliance officer
- Head of Marketing

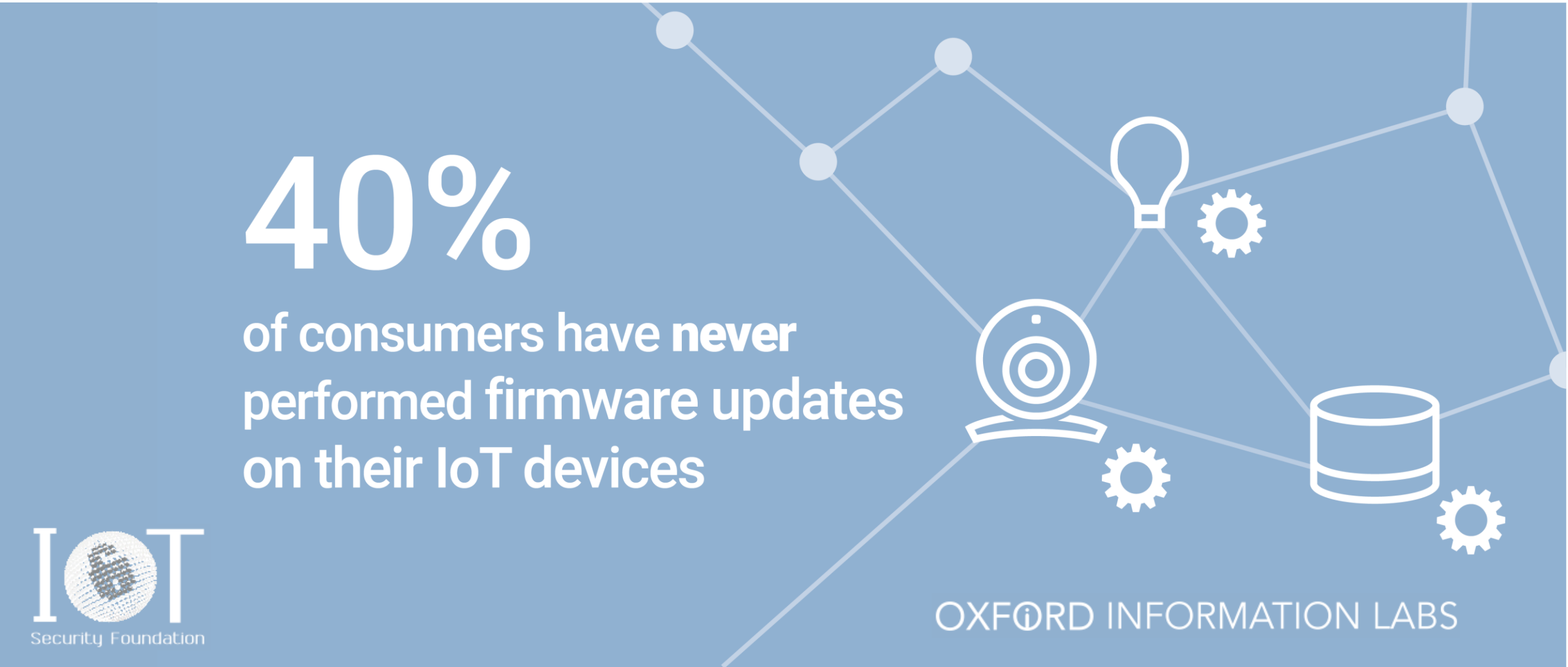
IoT Security Foundation

OXFORD INFORMATION LABS

Meet the presenters

Standards and regulation

What is the problem with software updates?



Standards and Regulatory Change

Standards

- ETSI EN 303 645 Consumer IoT cybersecurity

Regulation

- US: California Senate Bill #327, Oregon House Bill #2395
- UK: Proposal for regulating consumer smart product cyber security (summer 2020 – consultation on draft legislation)

IoT Security Foundation

OXFORD INFORMATION LABS

What guidance is available?

- Subject-specific guidance
  - IoTSF Quick Guides
  - IoTSF Best Practice Guides
  - ENISA
  - US NTIA and NIST

Codes of Practice

- UK: Code of Practice for Consumer IoT Security
- Australia: Draft code of practice

IoT Security Foundation

OXFORD INFORMATION LABS

ETSI: Cybersecurity for Consumer Internet of Things Baseline Requirements

ETSI EN 303 645

- First international standard of its kind
- ”Brings together widely considered good practice…baseline provisions.”
- “As consumer IoT products become increasingly secure, it is envisioned that future revisions of the present document will **mandate** provisions that are currently recommendations”

Legislation is making these provisions mandatory

IoT Security Foundation

OXFORD INFORMATION LABS

ETSI standard – in brief

Top 3 Covered in this webinar series:

- No universal default passwords
- Implement a means to manage reports of vulnerabilities
- **Keep software updated**

Others:

- Securely store sensitive security parameters
- Communicate securely
- Minimize exposed attack surfaces
- …And more!

IoT Security Foundation

OXFORD INFORMATION LABS

UK proposed regulation overview

Aim: Establish a cybersecurity baseline for consumer IoT products

What does it say *now*?

- Applies to network-connectable consumer IoT products
  - “has one or more network interface that can receive and/or transmit digital data”
  - Consumer market, but could be used by businesses
- Sets out obligations for IoT producers and duty of care for distributors
- Products that do not comply should not be ”supplied or made available to consumers” on the UK market

Failure to comply?

- Fines or removing products from the market

Requires transparency on how long the product will receive security software updates

Security update support period…

- Define a minimum amount of time
- Published
- Accessible, clear, transparent

Why?

- Updating products is a key mechanism to resolve vulnerabilities or fix bugs
- Without update mechanisms, the security of your product will decrease over time
- Not supporting security updates increases risks users, data, devices, networks
- Can impact businesses and business continuity

IoT Security Foundation

OXFORD INFORMATION LABS

How can this webinar and Quick Guide help?

- Software update process
- Software update standards
- Distribution and configuration

Look out for other resources in this series

Free! Webinars on Vulnerability Disclosure and Software Updates

Free! Quick guides to complement the webinar topics https://www.iotsecurityfoundation.org/consumer-iot/

VulnerableThings.com …a vulnerability disclosure platform for consumer IoT supply chain.

VULNERABLE THINGS

About FAQs Report Join Sign in

Report Vulnerability

Report a vulnerability with a 'thing' or device. Report anonymously or get public acknowledgement.

Join

Join as a member. Easily comply with disclosure requirements. Manage disclosures. Get help.

Consumer Internet of Things Vulnerability Disclosure Platform

Free to report vulnerabilities. Join to manage reports and publish disclosures.

Report Vulnerabilities | Manage reports | Publish coordinated vulnerability disclosures | Access resources

Read more >

IoTSF Website: Manage Vulnerability Reports Quick

Twitter: UK Minister Minister for Digital Infrastructure

IoT Security Foundation

OXFORD INFORMATION LABS