Case Study: Smart Thermostat with Cloud Analytics

Business Context

- **Manufacturer:** SmartHome Tech Ltd.
- **Product:** Intelligent thermostat with predictive heating/cooling
- **Cloud Service:** Real-time analytics platform for energy optimization
- **Market:** EU residential and small commercial buildings

Key Challenge

- Product relies on cloud for core functionality (remote control, analytics, AI predictions)
- CRA requires compliance for both device AND essential cloud services
- EUCS certification needed for cloud platform to support CRA compliance

EUCS Implementation: Scope Definition & Subservice Assessment

Define Scope

- **Infrastructure Capability:** Virtual servers, storage, networking for data processing
- **Application Capability:** Analytics algorithms, user interface, mobile app backend
- **Data Flow:** Device → Cloud → Mobile App/Web Portal

Assess Cloud Subservices

- **Primary Cloud Provider:** AWS/Azure/Google Cloud (infrastructure)
- **CDN Provider:** CloudFlare (content delivery)
- **Third-party APIs:** Weather services, energy pricing data
- **Analytics Engine:** Potentially separate ML/AI service provider

Documentation Required

- Map each subservice dependency and security controls
- Verify existing certifications of subservice providers
- Identify security gaps requiring additional controls

Documentation and Assessment Process

Complete Annex F Application

- **Service Description:** Analytics platform capabilities and boundaries
- **Control Mapping:** Each Annex A requirement mapped to implemented controls
- **Subservice Controls (CSOCs):** Document inherited controls from AWS/Azure/etc.
- **Customer Controls (CCCs):** What thermostat users must configure
- **Evidence:** Policies, procedures, technical configurations, audit logs

CAB Coordination

> - **Select Accredited CAB:** Choose based on cloud expertise and EUCS accreditation
> - **Assessment Level:** Substantial (medium-risk IoT application)
> - **Timeline:** 3-6 months from application to certificate
> - **Audit Process:** Document review, technical testing, on-site assessment

Customer Responsibilities and Maintenance

Document CCCs (Examples)

- **User Account Security:** Strong passwords, MFA setup
- **Network Configuration:** Secure home WiFi settings
- **Privacy Settings:** Data sharing preferences and consent
- **Device Updates:** Installing firmware updates when available

User Guidance Provided

> - Setup wizard with security best practices
> - Regular security reminders via app notifications
> - Clear documentation on shared security responsibilities
> - Support channels for security-related questions

Maintain Compliance

- **Quarterly Reviews:** Monitor subservice compliance status
- **Annual Reassessment:** Formal CAB review of changes
- **Incident Response:** Coordinated handling of security issues
- **Certificate Renewal:** 3-year cycle with ongoing maintenance

Казус: Как CRA ще повлияе на производител на умни IoT устройства

(Case: How CRA Will Affect Smart IoT Device Manufacturers)

CRA Requirements for Manufacturer

- **Risk Assessment:** Comprehensive cybersecurity risk analysis for device + cloud
- **Technical Documentation:** Detailed security measures for entire system
- **CE Marking:** Demonstrate compliance for complete product (hardware + software + cloud)
- **Support Period:** Minimum 5 years of security updates for both device and cloud platform
- **Vulnerability Management:** Coordinated disclosure process with cloud provider

New Obligations

- **Essential Requirements:** Must meet Annex I cybersecurity requirements
- **Conformity Assessment:** May require third-party assessment for critical products
- **Incident Reporting:** Report exploited vulnerabilities to ENISA
- **Documentation:** Maintain comprehensive technical files throughout product lifecycle

Practical Implementation Roadmap

Phase 1 (Months 1-3): Preparation

- Gap analysis against CRA and EUCS requirements
- Select and engage CAB for EUCS certification
- Begin Annex F documentation

Phase 2 (Months 4-9): Certification

- Complete EUCS assessment and certification
- Finalize CRA technical documentation
- Prepare for conformity assessment

Phase 3 (Month 10+): Market Launch

- Product launch with CE marking
- Ongoing compliance monitoring
- Customer education and support

Key Challenges

- **Coordination:** Aligning device and cloud security measures
- **Documentation:** Comprehensive technical files and evidence
- **Ongoing Costs:** Maintaining certifications and compliance
- **Customer Education:** Ensuring users implement required CCCs

Presenter Notes

Slide 1: Introduction

Start with the business context to help audience understand the real-world scenario. Emphasize that this is a typical IoT device that many companies are developing.

Slide 2: Scope & Assessment

Focus on the technical complexity - this isn't just about the device, but the entire ecosystem including subservices.

Slide 3: Documentation

Highlight the documentation burden - this is often the most time-consuming part of compliance.

Slide 4: Customer Responsibilities

Emphasize shared responsibility - customers have a role in security too.

Slide 5: CRA Impact

Connect back to CRA requirements and show how EUCS supports CRA compliance.

Slide 6: Implementation

End with practical next steps and realistic timelines for implementation.

> **Estimated Presentation Time:** 20-25 minutes with discussion
>
> **Recommended Format:** Interactive with Q&A after each major section