TESSOLVE

Cyber Security of Medical Devices

Tessolve - Leaders in Verification

Global presence in all high-end technology locations

Software testing	Hardware verification	Consultancy	Training

Levels	Domains	Tools
Unit	Web/Mobile	Test automation
Integration	Safety-related	Test management
System	Embedded	Coverage analysis
Acceptance	Security	Static analysis

Vertical Domains
- Semiconductors & FPGA
- Automotive
- Aerospace
- IoT
- Medical

TESSOLVE
A Hero Electronix Venture

Challenging Times

Navigating 21st Century

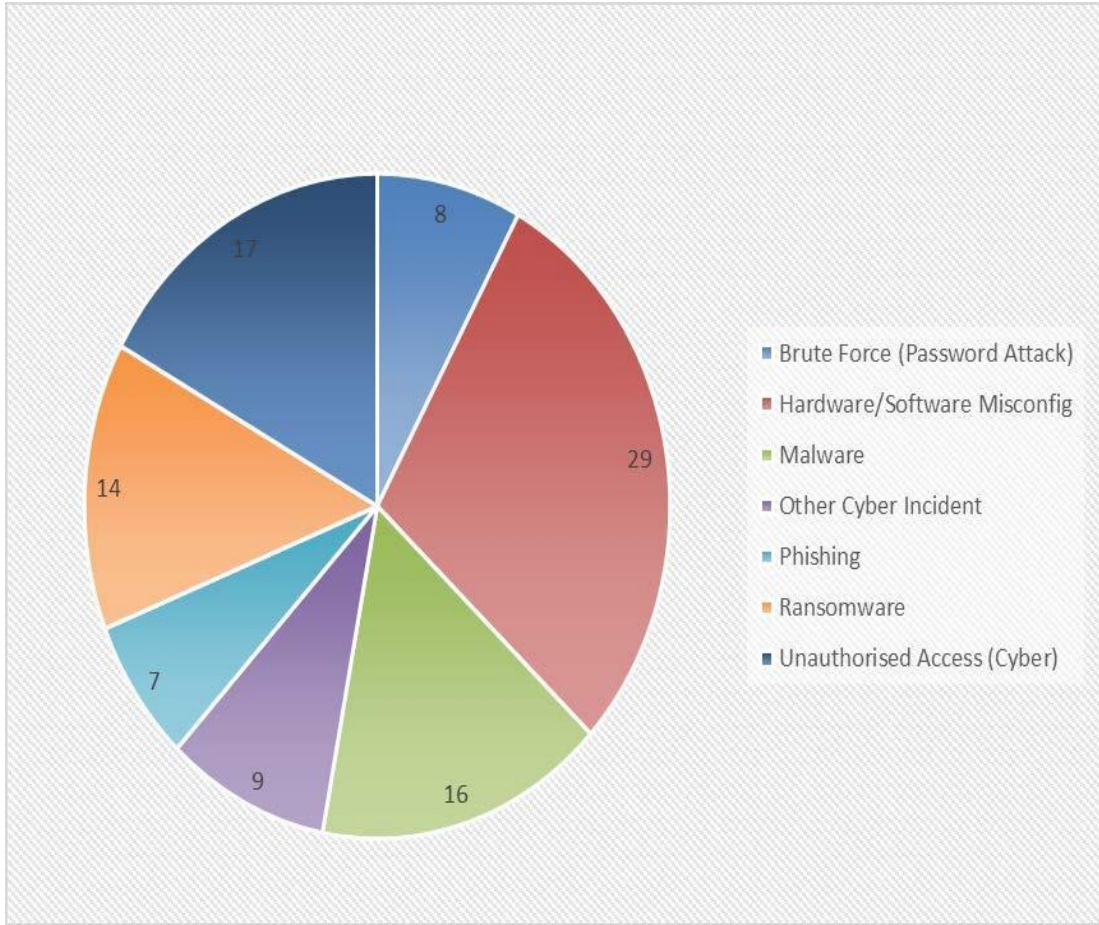
TESSOLVE
A Hero Electronix Venture

Increasing Threat

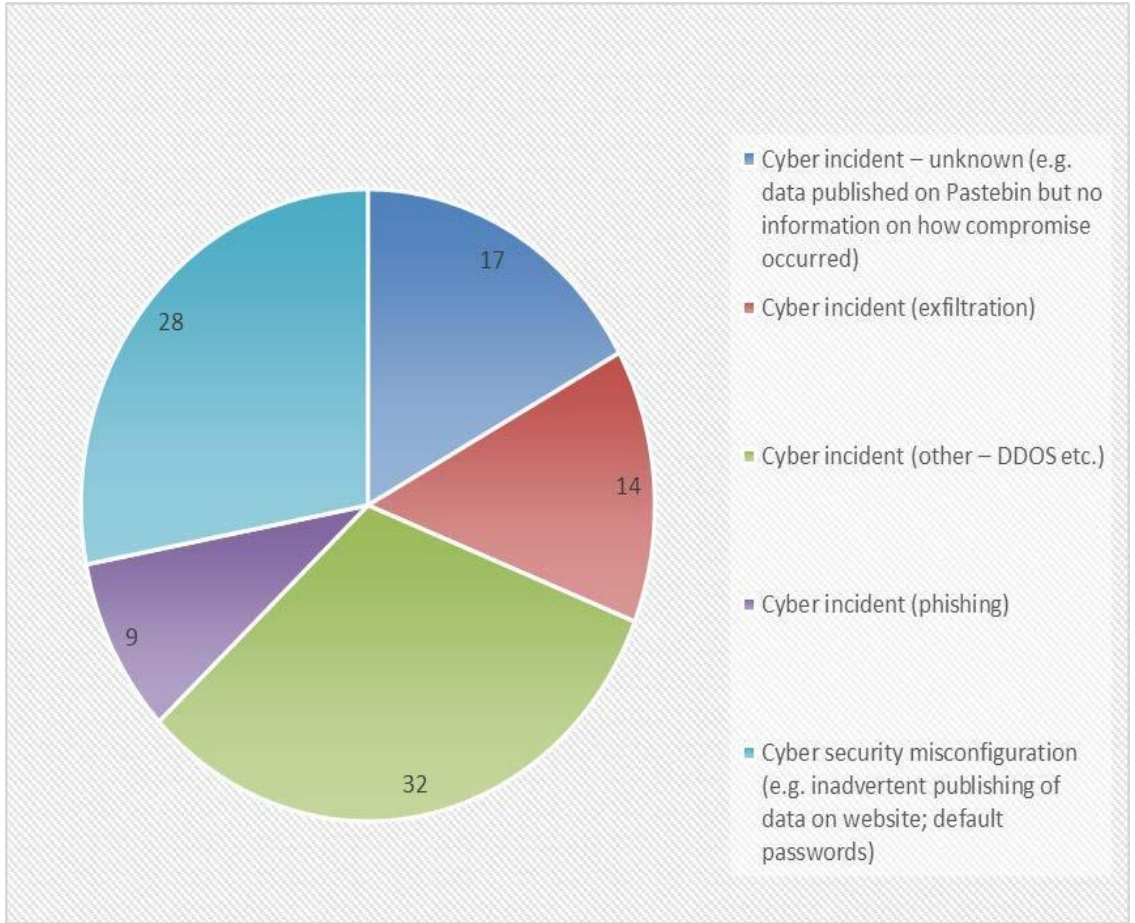
TESSOLVE
A Hero Electronix Venture

Evolving threats

Cyber 'old' breach type

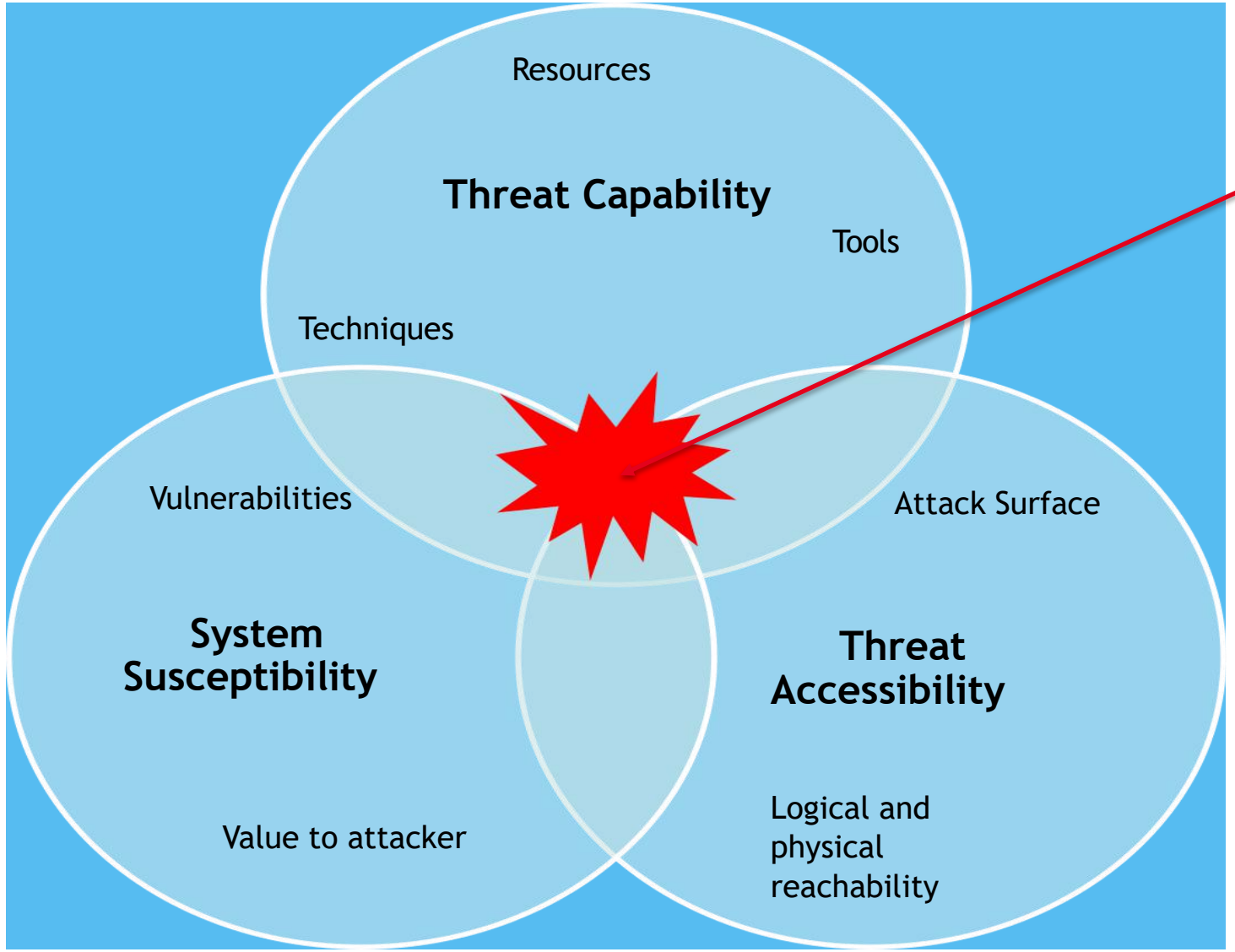


Cyber 'new' breach type



Source: ICO ORG data trends 2017= https://ico.org.uk/about-the-ico/news-and-events/news-and- blogs/2017/09/data-security-incident-trends-q1/

Threat Assessment



Successful Attack

GDPR Impact

Accountability, responsibility, and the ability to demonstrate data privacy plans & implementations

Article 25 - Data protection by design and by default	• Implement appropriate technical and organizational measures, such as: • pseudonymisation & data minimization • integrate the necessary safeguards • only personal data necessary for purpose of the processing
Article 32 – Security of processing	• Pseudonymisation & encryption of personal data • Ability to ensure the confidentiality, integrity, availability and resilience • The ability to restore access to personal data in a timely manner • A process for regularly testing, assessing and evaluating
Article 33 - Notification of data breach to authority	• In the case of a personal data breach, the controller shall without undue delay notify the personal data breach to the supervisory authority
Article 34 - Communication of data breach to subject	• If personal data breach is high risk, the controller shall communicate the personal data breach without undue delay. • The communication not required if the controller has implemented appropriate technical protection measures
Article 35 - Data protection impact assessment	• If using new technologies is likely to result in a high risk, the controller shall carry out an assessment • The assessment shall contain at least the measures envisaged to address the risks, including safeguards, security measures

Why are Medical Devices Vulnerable

Why are Medical Devices so vulnerable?

Connected devices create an increased level of intrusion, generating new types and unprecedented quantities of data, raising potential quality and security issues.

Connectivity Standards

onem2m	Open Interconnection Consortium	Wireless IoT forum
IETF	ZigBee Alliance	Industrial Internet Consortium
ITU	AllSeen Alliance	GSMA
ISO/IEEE 11073	AllJoyn	Thread

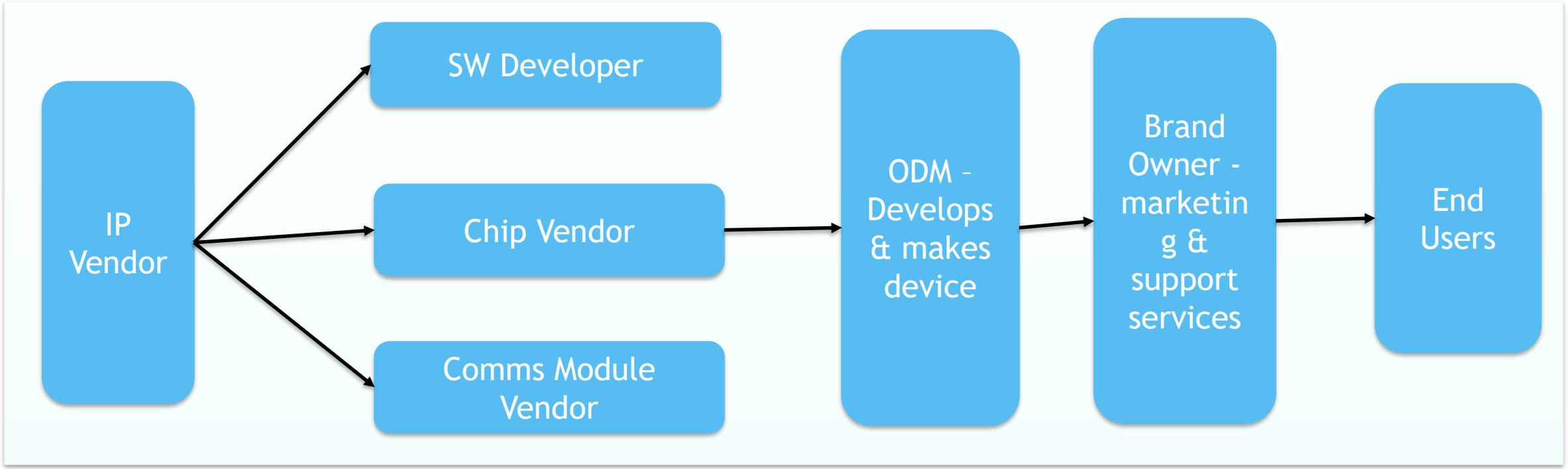
Security

- Window of opportunity - upgrades to software must be approved by the manufacturer, resulting in delays.
- Medical devices often operate withcommercial CPU, operating systems, or off-the-shelf software.

Quality Assurance

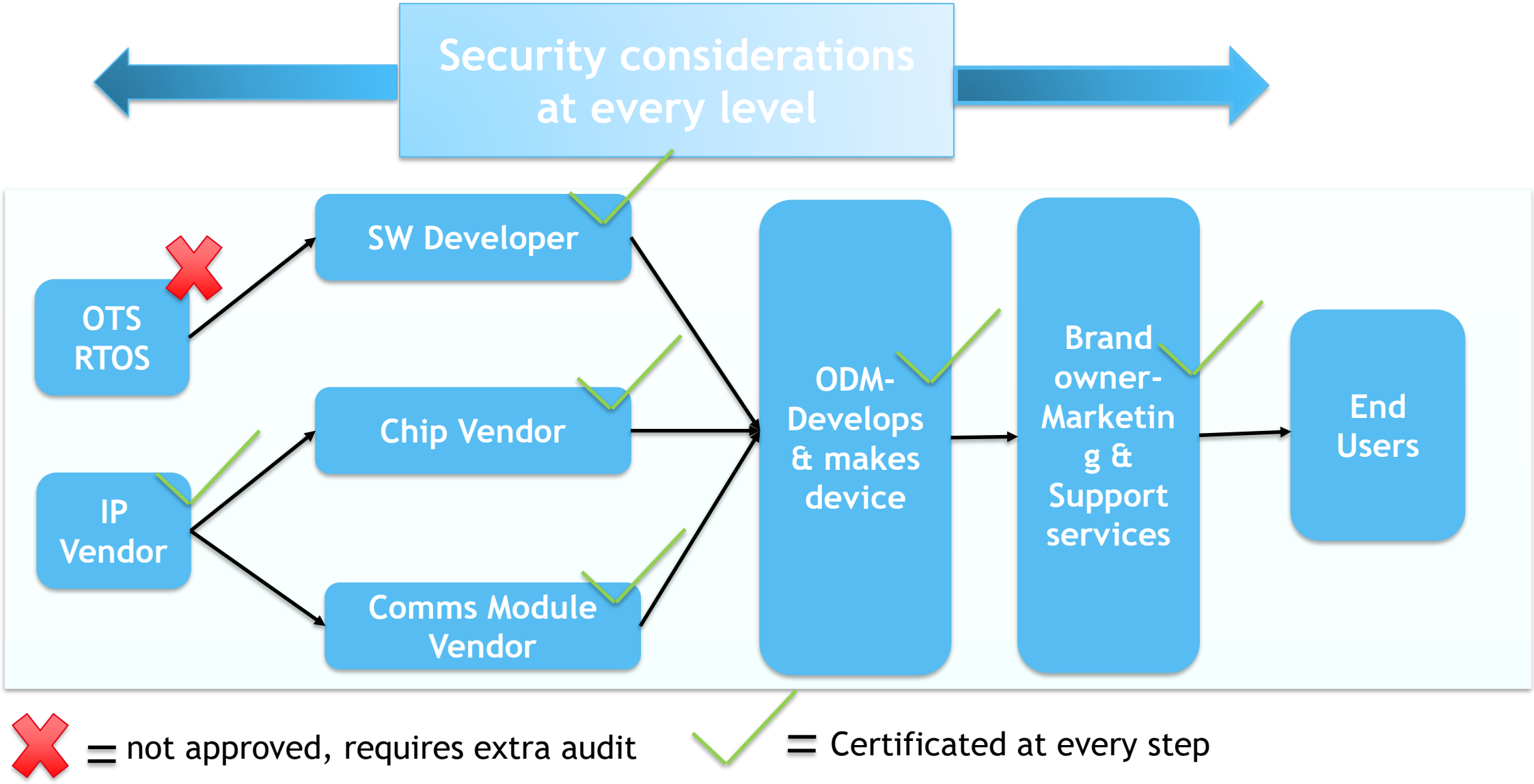
- Device operating systems are often early generation and may no longer be supported.
- Quality Issues within a Complex Supply Chain

Complex Supply Chain



1. Self Certification scheme
2. Connected products
3. Patching constrained devices
4. Framework for vulnerability disclosure
5. IoT security landscape

Trusted Supply Chain



Ongoing Patching & Maintenance

Devices require functionality and security updates

- **Patching devices is not easy:**
  - It gives another route to install malware
  - Regulation may slow down patching allowing window of opportunity
  - Devices have limited resources (CPU, memory, encryption, etc)
  - Functional issues (e.g. losing power during a patch can “brick” a device)
- **Responsibility**
  - Manufacturers? Consumers?
  - Who is going to pay for a lifetime patching warranty?

Kitemarks & Confidence in Medical Devices

TESSOLVE
A Hero Electronix Venture

Standards bodies – building TRUST

- **Example - BSI (British Standards Institute) attempts to build TRUST with consumers**
  - Can we build standards that guarantee some level of confidence
- **Do we need different levels of confidence?**
  - Heart monitor vs. doctor app booking vs. calories intake
  - In safety systems we start with a hazard analysis
    - From that we can set an integrity level
    - And that implies different levels of development practices
- **The NMI prefers levels of sign off**
  - Self- certification
  - External certification
  - Independent certification
  - Full certification against industry standards

Medical Device Kitemark Model

	Network connectivity - (1)	End 2 end security - (2)
Purpose	ensure solutions verified against a wide range of networking connection / connectivity protocols	ensure solutions verified against a wide range of security conditions and scenarios
Standards	• GSMA IoT connection efficiency guidelines • onem2m connection standards	• GSMA IoT security standards • Onem2m security standards • OWASP Internet of Things Top 10 • Online Trust Alliance's IoT Trust Framework
Example scenarios	1.) minimize the number of network connections. 2.) cope with variances in network data speed and latency considering 3.) communication requests fail. 4.) Communication retry mechanisms implemented verified.	1.) Authentication / authorization eg interfaces disallows weak passwords. 2.) Encryption model eg HTTPS. 3.) Cloud interface has account lockout 4.) Software / firmware. Eg Ensure all devices operate with a minimal number of network ports active.

Tessolve Medical Device 360 Security Testing

TESSOLVE
A Hero Electronix Venture

360 Security Solutions

- **Tessolve Application Security Testing services bridge the crucial security gap between perimeter defenses and penetration testing**

- **Solutions**
  - **Application Security**
  - **Security by Design**
  - **Security by Coding**
  - **Security by Testing**
  - **Coaching over training**
  - **Targeted Penetration Testing**
  - **Application Sensors**
  - **Code Scanning**
  - **Manual code inspection**
  - **Outsourced Testing**

graphixasset
Thinking technology

GraphixAsset award-winning, UK based, software and digital solutions provider. Developed eMAR system specifically for a national charity, providing services for people with learning disabilities throughout England.

Tessolve asureSECURE team tested:

- Functional / Usability & Security Testing of the Android application, Web application and APIs
- eMAR application's defence against an unauthorized attack and identified vulnerabilities. (Utilising OWASP)

Penetration Testing Services

Web & Application | **Device & IoT** | **Network & Infrastructure**

- **Experts take care of highly technical tests and work with your project teams to investigate those hard-to-find vulnerabilities**
- **Penetration Testing Report that includes detailed information:**
  - **identified risks**
  - **vulnerability findings**
  - **an action plan to apply fixes.**
  - **post-exploitation (clean-up) work such as removing traces, backdoors, and deleting logs will also be conducted**

Example Penetration tests

Social Engineering	• Make a person reveal the sensitive information like password, business critical data • Human errors are the main causes of security vulnerability
Web application	• Verify if the application is exposed to security vulnerabilities
Physical	• All physical network devices and access points are tested for possibilities of any security breach
Network	• Openings in the network are identified through which entry is being made in the systems
Remote access	• Login to the systems connected through these modems by password guessing or brute forcing
Wireless Security	• Discovers the open, unauthorized and less secured hotspots or Wi-Fi networks and connects through them

Mobile Security Management

Helping healthcare providers to reduce mobility management spending

42Gears Enterprise Mobility Management Solution:

- Secure, Provision, and Manage deployed devices
- SureLock restricts device usage and allows access to only business applications
- SureMDM provides centralized management capability of field devices.

Data privacy Services / GDPR

Be Ready for the General Data Protection Regulations (GDPR)

- Vrisk/Privacy impact assessment
- Regular Penetration Testing
- Compliance Documentation and Support
- Virtual Data Protection Officer

Summary

- Increased regulation
- Focus on QA & security
- Kitemark & Certification model
- Rebuild trust
- Marketing of secure devices

Unless these issues are addressed the only winners in the cyber wild west will be the hackers.

Thank you for your time

Team Tessolve

TESSOLVE

Contact- sales@tessolve.com