DIRECTinsight
directinsight.co.uk

The EU Cyber Resilience Act

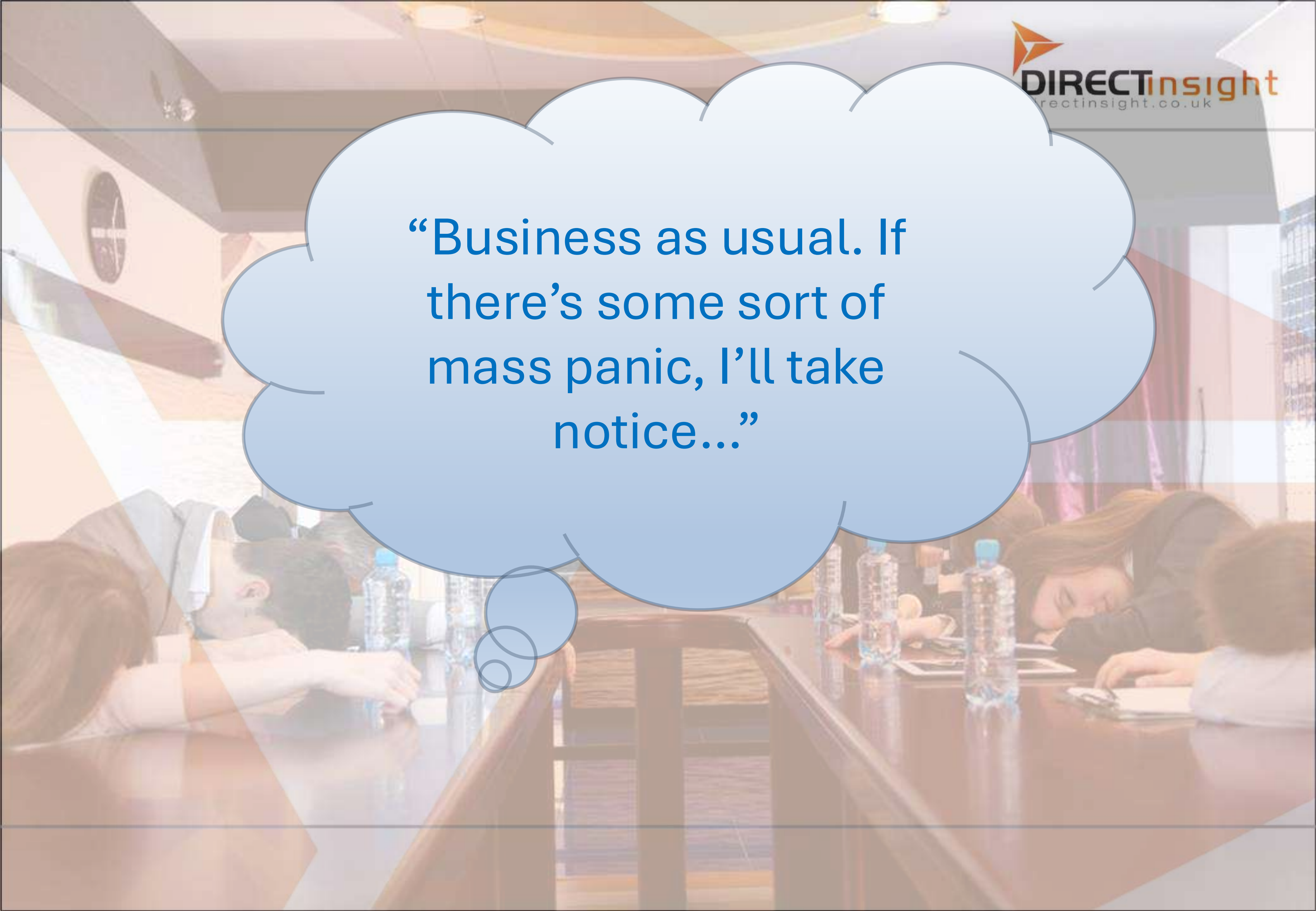
Implications for Embedded / IoT Developers

David Pashley
Direct Insight Limited

Plan A
Plan B
Result
Result
Time
Money
Quality
Market

“Just another piece of Euro-waffle that will pass me by...”

“We’re not even part of the EU so I don’t need to worry…”



“Business as usual. If there’s some sort of mass panic, I’ll take notice...”

Reasons to sit up and take notice

- Which ever way you look at it, cybersecurity standards are coming
  - King’s speech included “Cyber Resilience and Security Bill”
- A secure product is what your customers want, after all
  - While you’re looking for excuses, your competitors are getting on with it
- No CRA compliance = no CE mark
- 3 year deadline

Requirements

- “ship without known vulnerabilities” -> via documented process
- “ensure that vulnerabilities can be addressed through security updates” -> Guarantee to update against all future CVEs
- “provide for mechanisms to securely distribute updates” – OTA updates, f.o.c. for lifetime (min. 5 years)
- “authentication” + “secure by default configuration” -> Secure Boot mandatory
- “encrypt data at rest or in transit” -> Encrypted FS andTLS
- “identify and document vulnerabilities and components by drawing up a software bill of materials (SBOM)”. -> Provide, analyze SBOM

Implementation issues

Many requirements can potentially be met retrospectively

– But it might be messy

Some probably can’t:

- OTA updates
- Authentication via secure boot
- Encryption

System redesign required

- Read more:

https://blogs.directinsight.co.uk/eu-cyber-resilience-act-101-for-embedded-developers/

Thank you!

…and a quick mention for Direct Insight

We're already working alongside our customers to develop CRA-compliant hardware, software and systems.

If you need to do this, we can probably help.

If you are wondering whether you can achieve compliance retrospectively, we can help you to review.

Example customer platforms

Defence / scientific

Soldier Tracker

National Oceanographic Autosub

("Boaty McBoatface")

Point of Service

POS Terminal with NFC

Wireless Theatre Device

Example customer platforms

Medical

Industrial

Transportation

Cardiac Trigger Monitor

Energy and Resource Monitoring

Rail Condition Monitoring

Charge Post

DIRECTinsight
directinsight.co.uk

The EU Cyber Resilience Act

Implications for Embedded / IoT Developers

David Pashley
Direct Insight Limited