Follow on from Product Liability panic

On reflection

Purely speculative position. Given the lack of definition, and the conflict between the headlines and the counter headlines. It would be reasonable to conclude that – This is supposed to be for consumer products. The wording is possibly ambiguous to prevent consumer product manufacturers claiming “professional” application. This of course would be an all to easy escape, and would potentially leave an open exit to not well-intentioned manufacturers.

I suspect it is purely for this reason that the law reads the way it does. It may be imperfect, but much primary legislation is! This was why I sounded a slightly positive note on UK legal system. There will be “case law”, and this kind of legislation is not without precedent. Examples of this kind of law are Tax Law, and Health and Safety Law (in the UK). Tax law is generally strict liability, its so complex that it is heard in specialist courts, it is judicially fair – one need only look at the number of times HMRC lose in court to see that they are definitely not Judge Jury and Executioner! The independence of the judiciary is maintained in this field, and there is no evidence to suggest that the same course will not be followed.

If we assume that this will be the path – what should we consider?

Strict vs Absolute Liability

Strict liability does not mean “no defence” much in the poorly oversimplified way we were all told at school “in the eyes of the law, ignorance is no defence”. Whilst true, it is presented in a somewhat knowingly misleading way. Much as the “I am only responsible for what I say, not how you understand it” is the weakest of all statements, and in my view somewhat pernicious! I prefer to have my peer in conversation to be fully cognisant of the implications, and will take lengths to ensure (much to their eyerolled boredom) that they do have an accurate expectation. Its not “thrilling” but, its arguably more responsible.

We move to “reality”. If you broke some arcane law in ignorance, yes, you may well be strictly guilty. You did a thing, that was illegal, you didn’t know it was illegal, you demonstrated that if you had know it was illegal, you wouldn’t have done it. This will work in your favour, not in guilt or non-guilt, but as a matter for serious consideration when punishment is assessed. As opposed to absolute liability, which may have a defined punishment, and there are fewer mitigating arguments. This now comes down to “due-diligence”.

My takeway on consideration, and from my limited perspective is. “The sky isn’t about to fall on our heads, we will carry on.” Here are my thoughts on how we demonstrate that we are being careful.

Documentation and implementation

In order to give “state of the art”. I try to create systems that stand a low chance of failure. In my non omniscient human posture, I cannot claim this to be exhaustive. However, these common practices help to demonstrate that I am not being negligent, but in the context of “there is always more that can be done”.

Things I don't like, and how I remove them

- Lights going off and speakers going silent
  The simplest way to prevent this is to stop any interference with the control, and media network planes.
    - Segment the network so that traffic is limited to where it is needed
        - This can be by Layer 2 VLANS
        - This can also be by Layer 3 IP Subnets
        - Often – both
    - Deploy suitable access control
        - Automatic assignment of networks per device
        - IEEE802.1x via RADIUS can instruct network devices to execute the segmentation
        - Users (humans) that can interfere should be logged and allowed access on a least trust basis (ideally zero trust).
        - Credentials need to be unique and not vague – passwords don't do this well at all!
        - Better (where possible) is a framework that works WITH the access controller, using cryptographic keys.
        - Repudiation, is at least as important as Enablement – this means that a user that has "left" no longer has access. A Device that has been retired/left, cant gain access anymore either
    - Maintain simple logs
        - Who did what, when and where
        - Which things changed their function
        - What was the chain of causation?

The "logging" thing is or more correctly was a little controversial. In a professional deployment, I am confident that nobody goes to work to mess up the show! Whatever we may feel about our colleagues privately, I am sure that nobody will act maliciously. The 2025 clarification on GDPR for legitimate use, namely the Data Use and Access Act (DUAA) 2025. This removes the need for endless recitals under GDPR for those of us that just need to demonstrate due diligence, by holding log records.

I have kept my specific implementation details private. This is to prevent a breach of operational security. It also means I can change the specifics, when improvements and liabilities are identified – in the progressive world of software "bugs" are inevitable. If properly documented, and demonstrated to be reasonable answers to questions, at least we can all improve together.

Matters of resilience are unique to each installation, I have my perspective, and over the last 20 years, I've had the arguments, and changed my position many times. If you ever had a disagreement with me, and still felt like I didn't give you the "magic bullet" this was likely because, I didn't have sufficient evidence to tell you what you clearly wanted to hear, whilst telling you unequivocally that I felt you were wrong! My only defence – I did some shows… they seem to have worked. Would I do them differently today – 100% yes. Would have I have done them differently back then – probably not!