WE NEED TO FIX IT

While 'human error' is often blamed when things go wrong, the 'technical' part of 'sociotechnical systems' often escapes the spotlight. In this article, **Harold Thimbleby** outlines how hidden risks with digitalisation have far-reaching consequences – and how we can start to fix them.

KEY POINTS

- **Digital technology supports everything we do in safety-critical industries.**
- **There are also hidden digital problems that affect everything we do, and things will go wrong.**
- **IT-related problems can have significant consequences for justice, as well as safety and security.**
- **The formal qualifications and relevant experience required for system designers in safety-critical sectors are often not specified in the way that they are for front-line staff.**
- **We have to manage digital risks more effectively to prevent associated incidents and even miscarriages of justice.**

Digital problems are ubiquitous and can affect any of us at any time, even without us being aware of it. When things go wrong, especially when there are disastrous consequences, there will often be an investigation. This might be anything from an internal review, a disciplinary process, or even police investigations and criminal proceedings. In my experience in healthcare, too often investigations do not appreciate the central role that digital plays. Computer systems have sometimes been badly designed, failing to support what users need to do. Poor design encourages workarounds and errors, and computers can be buggy, causing further problems. There may be a cyberattack or unauthorised manipulation of data. Or data may just get 'lost'. These are all common scenarios.

"IT-related problems can have significant consequences for justice, as well as safety and security"

Computers and the courts

In some cases, IT-related problems can have significant consequences for justice, as well as safety and security. In 2015, one criminal case concerned alleged fabrication of patient data by two nurses at the Princess of Wales Hospital, in Wales. The Court determined that the evidence concerning IT systems was unreliable and was therefore excluded. As a result, the nurses were freed. This was only after *"enormous expense … incurred in trial preparation – hundreds of hours of time spent by experts, by the investigators, by lawyers"*, and after much court time, and much distress for the nurses and families of the patients concerned (England and Wales Court Ruling, 2017).

I got involved as an expert witness, and provided the evidence that established that the nurse's alleged "fabrications" could in fact be traced to the company that built the computer system (see the Court Ruling, also Thimbleby, 2018). An engineer had deleted patient records, creating the impression that the nurses had been fraudulent.

The key point of this story is that nurses, managers, internal investigators, police, lawyers and more, all failed to realise that the computer system the hospital was using was unreliable. Moreover, patient records had been modified by an outsider who had no authority to do so. From the first investigations in 2012 to reaching court in 2015, the hospital and the police had had years to think about it, but they still didn't realise.

This story is like the 'Post Office Horizon' case, where the UK Post Office prosecuted nearly 750 sub-postmasters and sub-postmistresses, averaging one prosecution a week, just on digital evidence based on logs from the 'Horizon' computer system (see Wallis, 2021). Many defendants were fined, lost their jobs, their homes, and ended up in prison; some, tragically, committed suicide. The Horizon case has been called the largest miscarriage of justice in UK legal history. The Court of Appeal held that the failures by the Post Office were an abuse of the process of the Court, and that the prosecutions were an affront to the conscience of the Court. It was established that some of the evidence concerning Horizon was misleading and other evidence was withheld.

The Horizon case is still going through appeals and has an inquiry under Sir Wyn Williams (2021), for which I am also helping provide evidence. We have asked the inquiry why it has not asked whether the developers of Horizon were competent to build such a system. It seems a silly question, but if accountants are giving evidence in court, you would automatically check whether they were qualified. So, wouldn't you also expect the programmers who are building complex accounting software that does accounting for thousands of Post Office staff to be competent in accountancy, overseen by accountants, or at least working in teams with accountants? I am aware of no evidence that such basic precautions happened with Horizon.

Both the Princess of Wales Hospital and Horizon cases ended up in court. One commonality between the cases is the Common Law presumption (of England and Wales) that a computer producing evidence is working properly at the material time, and that computer records are therefore admissible as evidence without question (Ladkin et al, 2020). In both the cases here, nobody questioned the quality of the computer systems, and the Court in the Horizon case forbade defendants access to it since it was presumed correct.

> "In both the Princess of Wales and Horizon cases, the many defendants were not aware of any computer problems when the prosecutions were brought"

This Common Law rule is nonsense when it is spelled out. Of course computers have bugs, and, just like human evidence, their evidence is no better than hearsay unless it can be audited back to independent evidence. Unfortunately, the Common Law presumption is applied blindly, though relying on it certainly avoids courts getting out of their depth discussing computer technicalities.

The lesson for us, therefore, is to try to avoid getting to court over a problem that was, or was partly, caused by computers. We must make sure incident investigators know the limitations of the police and the courts to sort out blame or culpability in digitally related or digitally induced incidents. More pointedly, we must try to make sure investigators realise that digital technology may have a central role in incidents until professionally proven otherwise.

Note that in both the Princess of Wales and Horizon cases, the many defendants were not aware of any computer problems when the prosecutions were brought. In hindsight, it might have been helpful to ask, "Is anyone else being prosecuted for the same alleged offence?"

Computers and competency

For the last four years, I've been writing a book on digital systems, and how we can see, understand, and solve associated problems. The book – *Fix IT: See and solve the problems of digital healthcare* (Thimbleby, 2021) – is about digital healthcare, but the same issues spread far beyond healthcare. All safety-critical industries have similar problems. (The book has a chapter on aviation.)

At the top of the left-hand page in the book (Figure 1), you can see a list of some of the many topics an anaesthetist must be qualified in before they can practise as anaesthetists. Including their general medical training, it takes about 14 years to train as an anaesthetist. They have to learn many medical topics, as well as topics in physics, human factors, and what to do in an incident. Once they've passed their exams and qualified, they are permitted to anaesthetise and treat patients with modern anaesthetic equipment, like ventilators, infusion pumps, anaesthetic machines, and more.

Almost all modern equipment has embedded computers, so when an anaesthetist uses anything, what it does to the patient depends on the quality of its programming. So the anaesthetist might decide the patient needs 5 mg of a drug, but it is the programmer who determines how much the patient actually receives, and how fast.

On the facing, right-hand, page of the book, you can see all the topics medical programmers are required to know before they can program medical equipment like ventilators. The publishers asked me if I'd missed out the details, as the figure in the book is completely blank. The fact is, there are no details to show, and that was the point of the figure. You can start programming medical apps, infusion pumps, or whatever you like with no qualifications or experience.

Some professions do have stricter rules. For instance, Air Traffic Safety Electronic Personnel (ATSEPs) require competence in providing and supporting air traffic systems, covering their specification, procurement, installation, maintenance, testing and certification. It's an

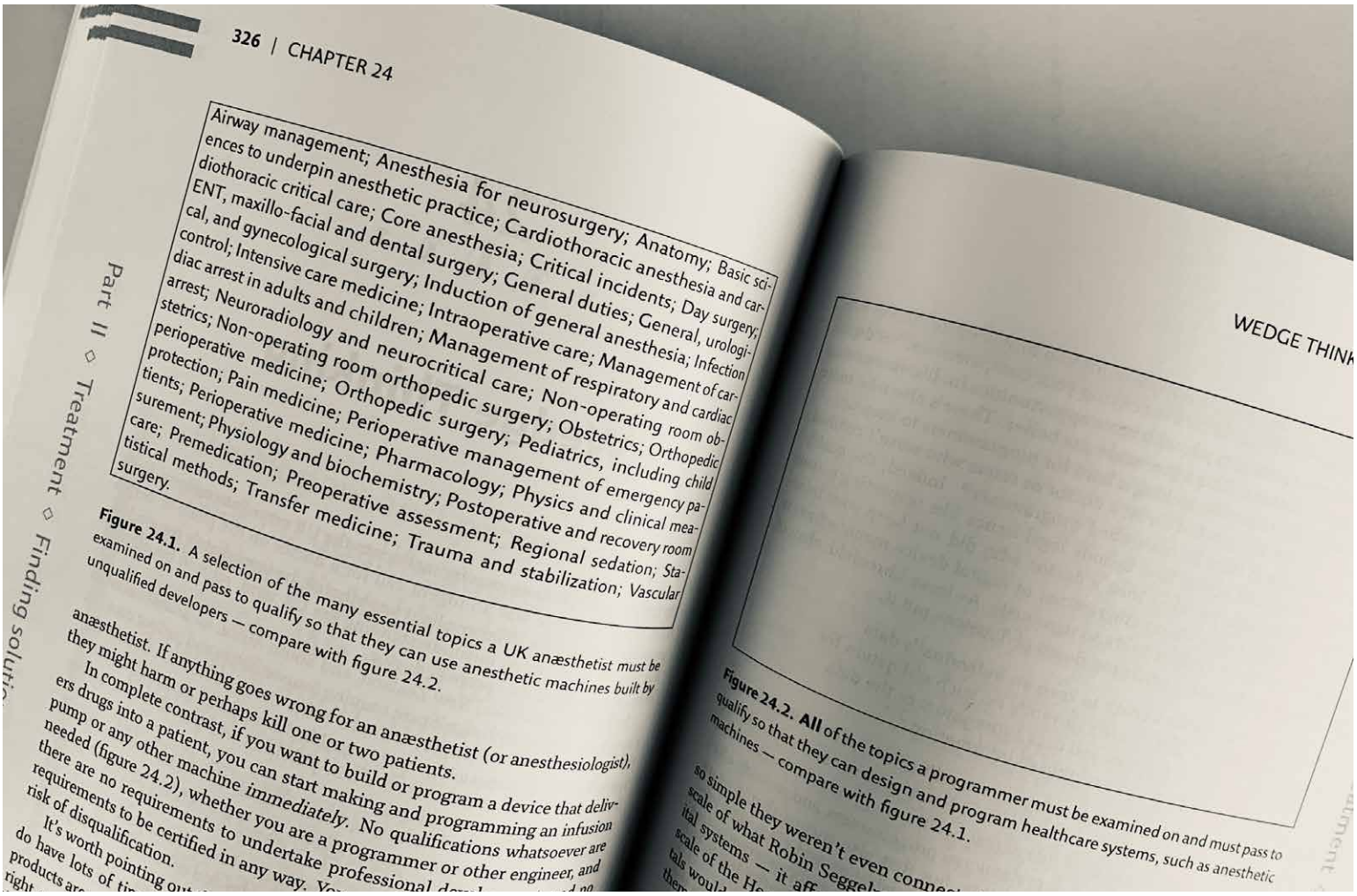

Figure 1: Formal knowledge requirements for UK anaesthetists and anaesthetic machine programmers.

improvement over anaesthetic safety, but it, too, places no requirements on the software developers.

In many areas of life, we must have qualifications, continuous professional development, relevant experience, and so on, before we are even allowed to work. There are generally rules about probation, supervision, etc. Yet increasingly, everything we do and what effect it has on the world is ultimately decided by digital systems. There are few rules to ensure these are designed professionally to assure safety. When things go wrong, then, the users are the only people who have apparently broken any rules, so they are easy to scapegoat.

Computers and cost

The digital systems you are using may have been brought in because they were cheaper than competitors and promised desirable solutions. Unfortunately, their programmers often have little idea about the skills and work of users. Users are often forced into workarounds to overcome the limitations of the technology. Things typically work after workarounds, so managers imagine things are working, and if anything goes wrong it must be a staff problem, not a technical problem.

We can learn a lot looking back to earlier periods of technical innovation. When Röntgen discovered X-rays in the late nineteenth century, they seemed like magic, helping to see broken bones, diagnose TB, and help during surgery. But ignorance, combined with enthusiastic overuse, resulted in many people getting cancer.

X-rays were very exciting when they were first discovered, just like digital is amazing now. Yet X-rays had risks that were not recognised, understood, or regulated – just like digital today.

"Digital has hidden intrinsic risks, and until we recognise them, errors and miscarriages of justice will continue"

So what to do?

If you thought the problem with any troublesome computers was that they're getting old, slow and obsolete, so you just need to get them updated with the latest innovations, you'd be wrong. Digital has hidden intrinsic risks, and until we recognise them, errors and miscarriages of justice will continue. So here are some recommendations:

1. If you are a front-line practitioner, record and communicate to safety professionals in your organisation how digital quirks cause unexpected, hidden problems for you or your colleagues.
2. Make sure that incident investigation teams include competency in software engineering and digital risk management.
3. Check that digital developers are suitably qualified and experienced, for the same reasons we require anaesthetists, radiographers, pilots, air traffic controllers, and other professionals to be properly trained: people rely on their competence to

keep people – customers, patients, passengers – safe.

4. Procurement must ensure new digital systems are dependable, and that developers properly engage with skilled front-line staff, before and after developing them. What standards were they developed and tested under?
5. Digital systems should be designed to anticipate failures using risk management expertise. Systems must keep auditable logs and double-checks of everything they do, so when incidents occur, reliable information is available to investigators.
6. If you are a manager, regulator, or policy-maker (or can influence one), try to turn any of these points into company policy or professional requirements.

It seems like a tough list, but digital technology is not well understood, and is changing every day. We must expect bugs when we are pushing boundaries. Cloud, blockchain, machine learning, artificial intelligence, digital signatures…no digital technology promoted today as an exciting, innovative solution has been around long enough to sort out its problems. Therefore, we must.

Professor Harold Thimbleby is a Professor of Computer Science and See Change Fellow in Digital Health, based at Swansea University. He's an Honorary Fellow of the Royal College of Physicians, the Royal College of Physicians Edinburgh, and a Fellow of the Royal Society of Medicine. Harold's work exposing problems in digital healthcare has stopped nurses going to prison.

www.harold.thimbleby.net

References

England and Wales Court Ruling (2017). Ruling in R v Cahill; R v Pugh 14 October 2014, Crown Court at Cardiff, T20141094 and T20141061 before HHJ Crowther QC, *Digital Evidence and Electronic Signature Law Review*, 14, 67-71.

Ladkin, P. B., Littlewood, B., Thimbleby, H. & Thomas, M. (2020). The Law Commission presumption concerning the dependability of computer evidence. *Digital Evidence and Electronic Signature Law Review*, *17*. https://doi.org/10.14296/deeslr.v17i0.5143

Thimbleby, H. (2018). Misunderstanding IT: Hospital cybersecurity and IT problems reach the courts. *Digital Evidence and Electronic Signature Law Review*, *15*, 11-32.

Thimbleby, H. (2021). *Fix IT: See and solve the problems of digital healthcare*, Oxford University Press.

Wikipedia (2021). *British Post Office scandal*. http://en.wikipedia.org/wiki/British_Post_Office_scandal

Wallis, N. (2021) *The great post office scandal*. Bath Publishing.

Williams, W. (2021). *Post Office Horizon IT Inquiry*. https://www.postofficehorizoninquiry.org.uk