Why I fear the NHS and BA computer meltdowns are a taste of worse to come, by security expert EDWARD LUCAS

By Edward Lucas for the Daily Mail

Published: 00:53, 30 May 2017 | Updated: 10:27, 30 May 2017

Cheap and convenient, but fatally flawed. That is the world we have created by our dependence on computers.

The £150 million compensation bill faced by **British Airways** for letting down tens of thousands of passengers over the bank holiday weekend is a reminder of what happens when we put too much faith in technology. The cost on this occasion was only in time and money. But as the cyber-attack on the **NHS** showed, if computers crash, lives can be at risk.

Far worse, I fear, is in store as we hurtle naively towards a fully interconnected world.

People checking in for flights at Heathrow also faced long queues on Sunday, as more flights were cancelled and delayed And it's not just the threat posed by countries such as Russia with a history of cyber-aggression, or rogue outfits such as WikiLeaks and Edward Snowden, the worker at America's National Security Agency who masterminded the biggest leak of state secrets in history.

On a more mundane level, security experts have proved that cars can be taken out of their drivers' control and crashed if the onboard computers are interfered with. In a similar way, medical devices such as pacemakers can be sabotaged remotely. Household devices including digital thermostats — part of the mushrooming 'internet of things' — are vulnerable, too.

Fraudsters

Our financial security is at severe risk, with internet banking a huge and easy target for fraudsters who can trick us into transferring money, or hack into our accounts and do it themselves. Meanwhile, countless daily online activities involve security systems that rely on sending messages to our phones, such as the authorisation codes that banks send to check an account-holder is indeed making a transaction.

Yet the international mobile phone system is alarmingly vulnerable. Its central software — SS7 — is easily breached, so an outsider might be able to read every message you send or receive. The result? A criminal can loot your bank account just as if they had your bank card and PIN.

Even those with valid bookings for Sunday were barred from coming inside the Terminal 5 building until 90 minutes before departure to avoid overcrowding.

But it's not our obsession with having the latest technology that is to blame. Believe it or not, some software used by the financial system in this country is so old, it still does its sums in

pre-decimal currency. Unsurprisingly, banks are reluctant to admit this and explain to the public why their systems are so outdated.

Gone are the days when we carefully checked cheque-book stubs against paper bank statements. Today, we believe what we see on the screen. But this is a paradise for criminals, pranksters and other enemies, who use the anonymity intrinsic to our computer systems to wreak havoc.

Why have we let this happen? It's simple. Since the invention of the internet, security has never been a priority. And our dependence on computers is increasing far faster than our ability to secure them.

In researching my book on computer security, Cyberphobia, I became increasingly horrified by the vulnerabilities I discovered we are creating. That said, even I would never have imagined a blue-chip company such as BA would build an IT system vulnerable to a single power failure. Nor that, in the safety-first world of aviation, it would fail to have a back-up system in place. Dozens more BA flights were cancelled from Heathrow on Sunday morning, adding to the passenger blacklog

Since the problem arose on Saturday, I have repeatedly asked BA to give me — a computer security expert — details of what went wrong. While blathering about a 'power surge', the company provides no real account of where it happened or why it caused such devastation.

Power surges — spikes in voltage — are highly unusual in this country, with its well-maintained electrical grid. The company's silence is as suspicious as its shaming inability to give a proper explanation to its passengers.

Flaw

Of course, part of our general problems with interconnectivity are technical. Modern software programs — the instructions that make a computer work — are too complex for any one person to understand. Inevitably, they contain flaws which remain invisible until something goes wrong and it is too late.

True, software companies make available program updates (known as 'patches') that help to prevent problems. But many users fail to install these. This was the case with the NHS cyber-attack. Hospital trusts were sent details of a security patch the previous month, but many neglected to update their systems.

This may have been because staff were too busy, or simply because they did not understand the need to keep their computers up to date. Alternatively, they may — rightly — have feared that by installing the patch they could cause something else to go wrong.

Thousands of British Airways customers were facing another day of chaos on Sunday as they queued out the doors at Heathrow in order to rebook flights cancelled on Saturday.

In that attack, criminals exploited a flaw in an ancient piece of software, Windows XP. Released in 2001, XP is now so old that Microsoft no longer bothers to issue updates. Most computer users have long since junked it in favour of more modern operating systems.

But many medical devices in the NHS, such as the MRI scanners vital for diagnostic images, work only on XP. There is another danger. Computers can send out spam email, or become part of a 'botnet' — an army of remotely managed computers that can be used to attack anything connected to the internet.

Against such threats, we need an equally formidable resistance. But we have nothing of the sort. Our legal and regulatory system, and our habits and attitudes, are woefully out of date, given our dependence on computers and networks. It doesn't help that discussion of the dangers is mostly cloaked in jargon.

Alex Cruz (51) was appointed boss of British Airways last year

But just as we can discuss road safety without needing to understand the physics of acceleration and braking, or the design of an automatic gearbox, it is absolutely vital that we get to grips with the online dangers we face.

The first principle to adopt is 'if you can't protect it, don't connect it'. Not everything has to be online. Already, some intelligence agencies are returning to paper records — typed with carbon-paper copies on mechanical typewriters — to reduce the cyber-attack risk.

True, electronic record-keeping brings convenience. Information is instantly available and easily copied or transported. But it also brings risks to the confidentiality, availability and integrity of the data. We need to make the price of carelessness more punitive.

Greedy

Next year, a new EU directive will come into force which subjects companies to hefty fines for data breaches. That is overdue and something Britain should keep, even after Brexit. Just as a restaurant chain would not survive carelessness with food, any user of computers should adopt high standards of technological hygiene.

But I am not optimistic. We as consumers — individuals, companies and governments — are greedy, impatient and lazy. We want the latest technology at the cheapest price, with the fastest communication and the least hassle.

We urgently need deep changes in the hardware and software we use — but also in the way we humans behave. Otherwise, the inconvenience BA's customers experienced this weekend is just a foretaste of the woes that await us all.

- Edward Lucas writes for The Economist.