The Millennium Bug – Reasons not to Panic

Ross Anderson

University of Cambridge Computer Laboratory
Ross.Anderson@cl.cam.ac.uk
11th December 1999

1 Executive Summary

There has been a lot of noise about the millennium bug, but little hard data. Many organisations have spent a fortune on the problem but refuse to share their findings. Governments tell their citizens not to panic while making panicky contingency plans in private. Few of the 'experts' in the field are willing to predict the outcome.

Here I report the results of an examination of the systems used in Cambridge University. The University is a federation of somewhat over a hundred and fifty departments, institutes and colleges which between them provide a very broad sample of small-to-medium sized enterprises. While colleges provide accommodation and catering services, our medical departments are involved in treating patients, our science laboratories operate major capital equipment and our aerial photography unit conducts flight operations. The sample may thus be more informative than a random sample of similar size.

The surprising discovery is that although some systems have been fixed or replaced, none of the bugs found so far would have had a serious impact on our business operations even if they had been ignored until January 2000.

So the UK government anxiety about the millennium bug compliance of small-to-medium sized enterprises appears misplaced. The average small business owner, who is doing absolutely nothing about the bug, appears to be acting quite rationally.

This does not mean that the millennium bug is harmless. There are still risks to the economy and to public safety, but in the UK at least they appear to be minor. This article recounts my own experiences; but when I talk to engineers who have worked with the bug elsewhere, they seem fairly typical.

2 Introduction

It is now well known that a number of computer systems will fail around the year 2000, as the transition from the year 1999 can cause time periods to be computed incorrectly. The press has been full of scare stories speculating on everything from the probability that someone making a phone call spanning the millennium instant will be billed for 100 years' talk time, to the possibility that the collapse of essential services will lead to riots, famine and widespread deaths.

2.1 First encounter

The 'millennium bug' problem has been brought to the attention of computer science students at Cambridge since the mid-1970s, but having studied mathematics and natural science as an undergraduate I first encountered the problem in 1986 when I was in charge of communications security for a clearing bank. The bank was in the process of tearing out an old ICL mainframe system and replacing it with the latest IBM equipment; the branch accounting software, which managed the bulk of customer accounts, was being rebuilt on a US software package, with thousands of small modifications to make it work the way local bankers were used to. My boss, the bank's computer security manager, observed that the accounting software package used only two digit dates and would thus start to fail in 1999. 180-day deposits would break 180 days before the millennium, followed by 90 day deposits and so on, until at the millennium itself even the current account system would fold.

He brought this to the attention of higher authority, and warned that after the bank had spent 1986-90 installing the new system, it would have at most four years to enjoy the benefits before it had to start ripping it out again.

The response was vitriolic: the bank's strategic direction had been approved by the Board of Directors, no change was possible, no opposition could be tolerated, and everyone would have to redouble their efforts to ensure that the chosen solution was a success. My boss resigned in February 1987. (As he predicted, the bank eventually had to spend a fortune fixing the problem: the package had been modified so much that a later, millennium compliant, version could not be installed until most of the bank's modifications were taken out.) I left some time after, and worked as an independent computer security consultant for a while before becoming an academic.

2.2 Skepticism

One of the things I did from time to time as a consultant was helping companies prepare disaster recovery plans. Back in the days of large mainframes, it was customary for a company to have two or more separate computer sites; one would do the production work, while the other was used for development, testing, and as a backup in case the production site suffered a fire, equipment failure or whatever. Companies that could not run their businesses at all if their computers went down – such as banks, stock markets and supermarkets – spent lots of money ensuring that they could recover smoothly from a failure within hours or even minutes. Arranging this can involve a number of tricky technical problems; it can be both interesting and lucrative for the consultant.

It was even more lucrative for the computer hardware companies, as it meant they could sell two mainframes instead of one. They therefore sponsored research on the subject. Many papers appeared which claimed that the average firm could not survive long for without its computers, and that only 20–40% of firms had properly tested disaster recovery plans. The authors of these papers concluded

that the average firm would not survive when a disaster struck, and often added that company directors were thus being negligent for not spending more money on disaster recovery services. The more honest of these papers were presented as marketing brochures for disaster recovery services [9], but many had the appearance of academic papers. Their effect was to create a consensus that disaster recovery planning was vital.

This was debunked in the early 1990's by the Bishopsgate bomb which wiped out the systems of hundreds of London firms. Some banks lost access to their data for days, as both their production and backup sites were within the 800 yard police exclusion zone [15]. Yet no firm was reported as going out of business. The later IRA bomb in London's dockland confirmed the pattern: it also destroyed a number of computer installations, yet companies bought new hardware and recovered their operations within a few days [5].

I mentioned all this in a 1995 paper on the design of highly resilient file stores [1]. But there was little academic followup. Computer security research tends to concentrate on confidentiality rather than availability, reflecting both the interest that people with a mathematical background often have in cryptology, and the priorities of the US Department of Defense which funds much of the research in the subject.

So by the time the millennium bug problem started to obtrude on the public consciousness in the mid-1990s, I found myself with two data points that were in tension with each other. On the one hand, a large and complex organisation such as a bank can be so dependent on its computer systems that it could be destroyed overnight if they fail, and I knew from long personal experience that making substantial changes to large mission-critical software systems can take years and cost a fortune. The history of large software projects is not encouraging; many are late and some are never finished at all [7]. So I expected that some large firms would not fix their software in time, and might have to close their doors. On the other hand, the more extreme Y2K predictions of 'TEOTWAWKI' ("The End Of The World As We Know It") brought to mind the claims made about disaster recovery planning by computer salesmen in the 1970's and 1980's. Thanks to the Irish Republican Army, I was inclined to be sceptical.

Nonetheless, the possibility of the millennium bug causing chaos and civil unrest was a factor in my decision, in 1996, to buy a secluded house in the country with a wood fired stove and a well.

3 1996–99: Growing Fear of the Bug

As the laboratory I work for is one of the world's leading computer science departments, and as I have responsibility for teaching and research in computer security and software engineering, I started to get asked from about the end of 1996 on what I expected to happen come the millennium. A particular concern was what to do in the health service; at the time, I was advising the British Medical Association about the safety and privacy of medical systems. For some

time, our Department of Health had been sending round circular letters saying that there could be a serious problem, but that it was up to individual hospitals and medical practices to deal with it, without any help from the centre.

3.1 International effects

I used my network of contacts to gather data. The immediately striking thing was the extent to which concern about the bug varied from one industry to another, and even more from one country to another. Here we had British companies such as BT and Unilever spending nine-figure sums on remediation, while their counterparts in countries such as Korea and the Czech Republic were doing nothing. As they used similar equipment and systems, they could not both be right! Either UK industry was being taken to the cleaners and the IT consultants were getting away with one of the biggest scams of all time, or a number of countries could look forward to severe disruption.

3.2 Electricity

The most critical utility is electricity, without which everything else stops. Indeed, during the 1970's and 1980's, the disaster recovery planning industry usually advised clients to provide two days' fuel for the emergency generator, on the grounds that the electricity was only likely to go off for longer than that if civilisation had collapsed. I hope that this does not turn out to be a self-fulfilling prophecy! Merely buying larger tanks will not help. A six-week power cut in Auckland illustrated that most emergency generators are not designed to run continuously for more than a few days, and businesses who used generators for the whole period of the power outage typically got through several of them.

As I had done some work for the electricity industry [2] I knew people there and asked around. I was struck by the diversity of opinion. Some experts reckoned that the central systems could be fixed easily, as they were under central control, but that embedded subsystems such as meters and switchgear in remote substations could not plausibly be fixed in time. Others reckoned the contrary – that the embedded systems would be easy but that the large, complex central systems such as power dispatching would be the critical vulnerability as they simply could not be tested in advance.

3.3 Healthcare

By the end of 1997, my practical concerns were focussed on the healthcare effects, including the effects of infrastructure disruption such as extended power cuts. These concerns grew as we received reports about likely failures of life-critical equipment [14] and heard from Dutch doctors about the much more thorough and early tests being done on hospital equipment there. They were brought to a head by a paper from the Medical Devices Agency, the government body

responsible for the safety of medical equipment. It stated, quite baldly: 'MDA believes that it would be irresponsible to set up any sort of general clearing house for information, since we could not verify information on numerous models and their possible variants, and it would be irresponsible to disseminate unverified claims that particular models are year 2000 compliant' [11].

After this shocking evasion of responsibility, Y2K issues started to be a significant theme in articles I wrote on healthcare informatics (e.g., [3]).

3.4 Can the government do something?

Although I have never aspired to be one of the 'experts' on Y2K, a number of organisations asked us for help. The Foreign Office wanted to estimate how the bug might affect them; I helped persuade them to order a survey of local Y2K awareness by British diplomatic missions overseas [8]. The result confirmed my initial assessment, that a significant part of the risk to the UK may come from unpreparedness in countries in Southern Europe, the Far East and the Middle East. This in turn led to the bug figuring in Prime Ministerial speeches at various international summits. The government also told the BBC to make a film about the bug, in which I duly appeared as one of the talking heads.

The government will still be exposed if the outcome is disastrous. Quite apart from the failings of specific departments and agencies, such as the MDA referred to above, overall responsibility has been visibly passed around. After the election in 1997 it went to a junior minister whose main responsibility was small business and whose secondary responsibility was introducing legislation to control cryptography. This led to government Y2K efforts being targeted at small businesses, and the responsible civil servant being in charge of the 'Electronic Commerce Bill and Millennium Bug Department' – he spent most of his time trying to persuade people that handing over their cryptographic keys to the intelligence community was a Good Idea. After a reshuffle in 1998, ministerial responsibility was passed to the Leader of the House of Commons; but she has no civil service support to speak of. There is a quasi-autonomous government agency – Action 2000 – but their attempt to advise people to stockpile a few weeks' supplies for the millennium was immediately slapped down by government PR flacks.

Sources suggest the main reason for this fragmented and indecisive approach is that the Treasury refuses to believe that the bug is a problem at all, and will not allow departments to spend enough money on it. If things go badly wrong, this excuse will not cut much ice with the electorate. On the other hand, if we have only a small-to-medium sized disaster, then Y2K may be the ultimate 'get-out-of-jail-free' card. It may end up carrying the blame for many political and administrative failings of a more traditional nature.

4 Cambridge University and Y2K

Like any other prudent organisation, Cambridge University set up a project to deal with the bug. The University has an annual turnover of £300m (about US$500m), assets of about £1bn, some 7,000 staff and over 15,000 students. It is highly decentralised, consisting of more than a hundred departments and institutes which do research and teaching, and about thirty colleges which provide accommodation and social facilities to students. It also owns a number of businesses of which two (the University Press and the Local Examinations Syndicate) are substantial. The main role of the central administration is setting overall policy and standards. It also provides some support services, such as accounting, payroll, site security and building management (except for the colleges, which perform these functions for themselves).

The University is thus an interesting test case for Y2K. On the one hand, there are large central financial systems similar to those of a big company or government department; on the other hand, almost all operational matters are down to the individual departments, colleges etc. These bodies undertake a very wide range of business activities. Staff at medical departments treat patients at two local teaching hospitals where they have most of their premises; our physics, engineering and materials science departments operate complex and dangerous capital equipment ranging from particle accelerators through gas turbines to superconducting magnets; our biological departments have large collections of specimens, some of which must be kept alive while others must be kept frozen; our colleges perform much the same functions as hotels; while humanities departments are like ordinary business offices in that staff use email and the web to gather information, create documents on networked personal computers, travel to conferences and so on. For more detailed information, see the University's main web pages [13].

At the beginning of 1998, a 'Y2K committee' was established, chaired by the Treasurer (our chief financial officer), and with representatives from a number of staff departments such as security, property services and the computing service. I sat on this committee as the teaching officer responsible for software engineering and thus the closest that we had to a 'Y2K expert'.

4.1 Initial assessment

In July 1998, we held a seminar to which representatives of all the University's constituent organisations were invited. At this seminar, I presented an initial assessment of the effect which the millennium bug might have on the University's external operating environment. The view I took, which was fairly typical of opinion at the time among engineers involved in Y2K work, was as follows.

1. There was perhaps a 5% chance of serious disruption at a national level. Examples could include a failure of the national power grid leading to outages

lasting longer than 48 hours; a failure of welfare benefit payment systems leading to social unrest; or a failure of the banking system. By saying the risk was 5% I was estimating only an order of magnitude; the interpretation was 'quite probably this won't happen, but the risk is there so it's worth making a contingency plan'.

2. There was perhaps a 15% risk of lesser but still significant disruption, such as of local utilities in some parts of the country but not others. I observed that while our local water company was spending some £30m on fixing the bug, a similar water company in the north of England was spending about one percent of that. Given that water companies were only recently privatised, I found it hard to believe their systems were different enough to justify this.
3. There was perhaps a 60% risk of disruption being caused indirectly as a result of business failures overseas. These might affect some UK businesses directly; a particular concern for Cambridge, with its large base of high-tech industries, might be a shortage of memory chips caused by infrastructure failures in the Far East. Previous computer industry experience suggests that a supply disruption for even a few months could have knock-on effects lasting several years[1]. However, I said that the most likely way in which overseas failures would affect Cambridge would be through an end to the current bull market in equities, as predicted by Yardeni [16].
4. It was always possible that the Y2K business would do no measurable damage to the economy at all. I rated the probability at 20% – 'quite possible but don't bet on it'.

I predicted that the greatest risk was where supply chains were either very long, as in energy, or very broad, as in civil aviation. In the latter case, for example, it had been pointed out by Martyn Thomas (then the Y2K practice manager for a large accountancy firm) that European air traffic volumes depend not just on air traffic control but on over two hundred other systems – fuel pipelines, spares inventory, passenger ticketing, baggage handling, bills of lading, customs clearance, and so on. If any of these failed, this was likely to reduce the amount of traffic that could be handled.

I pointed out that even if there is serious disruption in the first few months of 2000, the University has a secret weapon to survive it. We teach our undergraduates in three terms of eight weeks – Michaelmas Term from October to December, Lent Term from January to March and Easter Term from April to June. If Britain is in chaos in January, we can simply send the students home – in fact, if the electricity or water is off, health and safety regulations leave us no choice. But we can always shift the Lent term lectures to Easter, and the Easter lectures to what would otherwise have been the Long Vacation. This might have odd effects (e.g., May Balls being held in September) but was done on a number of occasions between the fourteenth and seveteenth centuries in response to epidemics of the plague. (On the last of these occasions, one of our grad students

[1] recent figures do indeed show a modest spike in orders for high-tech goods and electronic components [17]

was so bored with being stuck at home that he invented physics [12].) So there is a precedent – vital in a tradition-minded place like Cambridge – to reassure us that we can recover our teaching smoothly even after a national catastrophe.

This seminar was successful in motivating departmental Y2K officers to take the thing seriously. Over the next few months they were set to preparing an inventory of all their systems, identifying which were mission critical, and then either testing them directly or, where this was impossible or risky, seeking information on compliance from the supplier.

4.2 Detailed findings

Early this year, we got the returns back from the departments. Most systems were fine, while those with problems could be divided into five categories.

1. Most of the non-compliant systems can be fixed by manually resetting the date after the millennium arrives. The bulk of these are PCs, although there are also a few more specialised devices from geodimeters to pH meters.
2. There are a number of non-compliant systems whose anticipated failures 'don't matter' in the opinion of their users. One example is a 24-hour ECG recording device which will record the wrong date on the tape. Standard clinical practice is to have these tapes interpreted immediately afterwards and it is the resulting report, rather than the raw tape data, which is added to the patient's medical record: so the tape date doesn't matter. With other equipment, the clock has to be wound back a number of years, but the thing will then work fine so long as incorrect date outputs can be ignored.
3. There are a few systems which are 'none of your business'. For example, our technology departments have a number of scientific instruments which they built themselves and which need fixing, but which will inconvenience no-one but the researchers themselves if the fix is late. It is not appropriate for the central bodies to set priorities for research teams by telling them to fix old system X rather than building new system Y.
4. There are a number of systems which would have failed without software patches, but for which the patches have been delivered in time. Fortunately all major capital equipment affected by Y2K, such as NMR scanners, falls in this category. (This is hardly surprising as the suppliers would surely have been sued otherwise.)
5. Finally, there are some systems which will fail, which can't be patched and which have been replaced. The most expensive were several scintillation counters used in various clinical and life science departments, though we also had to replace two building access control systems and three intruder alarm systems, as well as upgrading our CCTV. (A further access control system – the one at my own laboratory – was fixed by a software upgrade.)

Any large collection of data will contain errors, and I do not claim our survey was infallible. For example, two instances of the same model of spectrophotometer were listed as 'compliant' and 'awaiting phone call from manufacturer' on the

same page of one department's return. But the great majority of the identified errors are best described as opportunism. Models of PC which were listed by one department as needing the date reset on the 5th January were listed by others as requiring replacement. One department even wanted a new microwave oven for its staffroom! (Our central authorities quite rightly took a jaundiced view of all this.) So I am fairly confident that the returns err on the side of caution.

The genuine Y2K problems – those in category 4 and 5 above – were mostly in our clinical and life science departments. This might appear to be bad news for hospitals, and I will return to healthcare below. But when we discount the systems for which the manufacturers provided patches anyway and look at the 'hard core', the category 5 systems, we find not a single one which, had it been left undiagnosed until the New Year, would have caused a catastrophe. In each case there was a workaround. For example, if an electronic building access control system fails, then an old fashioned metal door lock can be fitted in half an hour and faculty members can be given metal keys.

The one failure that caused us some worry is instructive. We have a central accounting system which departments use to pay suppliers for goods once they have been invoiced. In addition to being noncompliant, this system was rather elderly. Departmental accountants had long been asking for extra functionality, and the computing staff wanted to migrate to a newer generation of technology. A project was started to redevelop it, but ran into trouble; it became clear that the replacement could not be done in time. The old central system has now been patched up, but this has left us with a number of noncompliant systems in various departments whose owners had hoped that the central redevelopment would solve their Y2K problems for them.

This may be a good example of the sort of complex system problem that might conceivably put some firms out of business. However, it does not worry us much. There are many ways to deal with noncompliant departmental systems. One can run two instances of the old system on separate machines, one for purchase orders issued up until the middle of December 1999, and another which will start a new series of purchase orders in January 2000. This will be mildly inconvenient, as departmental accountants will have to deal with two systems rather than one for a short period; but it is not a big deal. (In extremis one can always go back to manual processing: our laboratory only raises 200–300 cheques a month.) This experience suggests that the typical modern, decentralised, organisation is pretty resilient – so long as interactions resulting from equipment duplication, timezones, reboots, rollbacks and so on can be managed.

Of course, we remain vulnerable to interruptions in essential supplies such as electricity and industrial gases. But had we done nothing at all about Y2K, we would not have been much worse off than we are now. It appears that the effort to date has been instructive rather than effective.

4.3 Lessons learned

So what lessons did we learn?

Firstly, the risk to which most small and medium sized businesses are directly exposed is pretty low. Most such businesses can revert to manual accounting overnight if they have to, and although there will be some firms that depend on a particular piece of capital equipment or a single large customer which might fail, they should be a minority. So I think that the government's efforts to get small business to 'do something' were misplaced. The average small business owner who has done nothing has probably acted quite rationally.

Secondly, even although many of the large complex central systems used by bigger businesses may not be fixed in time, this is not necessarily the end of the world. In many cases, there will be workarounds like those we found for our accounting systems.

Thirdly, most of the effort put into Y2K preparations was wasted. Where software was developed in-house, or its source code was available, then a reasonable assessment could be done; but for most systems, we were dependent on our suppliers. (Cambridge is a centre of expertise for reverse engineering embedded systems – see [4] – but although we could probably fix any given embedded system without the suppler's help, we do not in the end investigate a single one of them this way ourselves. Manufacturers offered bug fixes for all our really expensive systems and we did not have the motivation to investigate any of the others.)

Getting useful information from suppliers was a nightmare. There was an enormous paperchase of people writing to their suppliers seeking reassurance, and the resulting letters of comfort all seem crafted by lawyers to give no bankable assurance at all. ('We believe that all our systems are compliant but we can give no absolute assurances ... blah blah ... make no warranty about fitness for purpose ... blah blah ... like anyone else we are dependent on the continuation of electricity, telecomms and other utilities ...) Business schools might wish to study why little or no collective action was taken, even in those industries with statutory safety certification and a central body that might have done something – such as the Medical Devices Agency in the case of healthcare. It is clearly a bad thing that Britain's hundreds of hospitals, medical schools and clinical research institutes all had to write to the same equipment suppliers and deal with the same evasive, unhelpful answers.

5 So what may go wrong?

Against this background, what concerns remain?

5.1 Banks etc

The first of my remaining concerns is that some big companies will, like us, fail to fix their central systems in time but will not be able to find a workaround as we did. My experience working on disaster recovery plans for banks and stock

markets has exposed me to enough systems without which trading is simply impossible, and which might fail in ways which could not be fixed quickly. I hear rumours that at least one UK clearing bank is misleading itself, and thus probably the regulators, about its preparedness: this should surprise no-one who has worked in the industry. The usual IT management horrors, such as technophobic senior management and wishful thinking throughout an over-long command chain, ensure that chief executives often only hear about a software disaster just before it strikes. So it wouldn't surpise me if a big name company were to collapse, and if the victim is a bank then banking regulators might not be ready to take appropriate action. A traditional bank failure involves bad loans, dishonest management, a collapse of public confidence, or some combination of these; it is traditionally fixed by having the victim taken over by another, stronger bank. But if the victim no longer has working computer systems, this will be much harder.

Problems like these may be compounded in countries where awareness of the bug is low, and where monopoly utilities provide multiple single points of failure. Simultaneous breakdowns of banking, power, telecomms, water and other services might lead to civil unrest, government colapse and even opportunistic military action by neighbours. The possible impact on the UK economy of regional chaos in the Middle East or the Far East cannot be completely ignored. However, previous dates which the Y2K pundits claimed would cause widespread failure, such as 1/1/99, 9/9/99, M - 180 days, M - 90 days and M - 30 days have come and gone without even a ripple. This may give us some reassurance.

5.2 Panic by consumers

Another cause for concern is the possibility of competitive stockpiling.

In Britain, the Department of Health has instructed all general medical practices to make contingency plans for Y2K, but has drawn back from telling them exactly what to plan for. One practice with which I discussed Y2K issues decided that if serious disruption around the millenium is a possibility, then their priority was to provide for those patients whose lives depend on particular medical supplies.

A trawl through the patient database yielded the following.

1. The most highly dependent patients were two transplant patients needing a number of drugs, a dozen who needed oxygen for respiratory diseases, five who did dialysis at home, and one on parenteral nutrition. In the event of an extended power cut, the dialysis patients (at least) would most probably have to be hospitalised.
2. The largest single group of highly vulnerable patients was the diabetics. This practice has over a hundred, of whom over forty are insulin dependent and will die if supplies are interrupted. There are 370,000 patients who depend on insulin in the UK, plus a further million diabetics whose condition is controlled by diet and/or oral medication.

3. There are also several hundred asthmatics who depend on steroids and several hundred heart patients who depend on a variety of drugs. A failure of supplies for a month or two might cost twenty lives. Fortunately, most of the relevant drugs have long shelf lives (unlike insulin which only lasts a month or so outside a fridge).

The action taken by this practice was to start increasing prescriptions for most of these patients from 30 days' supply to 90 days'. But if all practices did the same, supplies would quickly run out. The pharmaceutical industry is resolutely opposed to drugs being stockpiled anywhere other than at the manufacturer, presumably out of concern that if stocks were built elsewhere and the feared disruption did not arrive, then destocking during January and February 2000 could undermine pricing arrangements in some markets.

It is well known to economists that the usual cause of famines is not an absolute shortage of food, but inefficient distribution – often caused by the fear of shortage leading to competitive stockpiling. The classic precursors of a famine appeared to be present in the pharmaceutical distribution chain. Not only might drug companies and patients compete to control the stockpile, but hospitals might also have been tempted to build stocks, as a supply breakdown would send desperate people flocking to the local hospital's accident and emergency department as the last resort. Stocks are often at a distance (much of Britain's insulin comes from factories in Denmark and the USA), so the supply is somewhat inflexible, and confidence could easily be eroded (for example, by chaos – or predictions of chaos – in air transport). Finally, there is no easy way for price fluctuations to clear the market in Britain, as most drug supplies to our health service are on long term fixed price contracts. So in early 1999, I was concerned that a panic might develop and the only way to deal with it might be temporary rationing. This has thankfully not happened – and as people typically have to wait six days for an appointment with their doctor, it seems too late for it to happen now.

Of course, there are many other sectors which might be affected by panic and competitive stockpiling; we had panics over petrol in 1974. But the only sector in which we can see any symptoms as of early December 1999 is high technology goods and in particular chips [17] – but even there, the spikes in demand are modest.

5.3 Panic by governments

I take no view here on whether critical central government systems (such as pension and welfare payments) will fail; all we've seen so far is a few weeks' disruption in the Passport Agency. The final concern I wish to raise is more subtle; it is illustrated by a UK government system called the 'Government Telephone Preference Scheme' or GTPS.

Under this scheme, all UK telephones apparently have a priority which is a single hexadecimal digit ranging from 0 (low) through F (high). Normal sub-

scribers are 0 through 9; GPs and JPs are A; police chiefs are C; while the highest grade of all, F, is reserved for phone company staff [6].

The cover story is that this is for congestion management: if the lines are too busy, the phone company can cut off progressively more of the subscriber base to maintain essential service. But with modern equipment, congestion management is done in other ways. The real purpose of the scheme is to control the population in the event of imminent revolution or nuclear war. It is a throwback to the 1950's and, although 'Civil Defence' was stood down well before the end of the Cold War, GTPS is still with us.

The scheme was last activated a few years ago after the IRA bombed the Aintree racecourse [10]. In theory only high-level scheme members should have been able to make calls[2]. It was a complete foul-up. One of the mobile networks kept on providing service (as the civil servants couldn't get through to them on the phone to tell them to switch off their customers) while the Army bomb disposal team couldn't use their mobiles as they'd forgotten to register them.

The scheme is now causing anxiety to health service staff. The government wants only doctors to be registered, but doctors want their nurses, receptionists and many patients on it too. Over the past few years, hundreds of thousands of people who used to receive in-patient geriatric care or warden controlled accommodation have been discharged and given alarm buttons so they can summon help instantly if they get into difficulty (e.g., fall and can't get up). There are also transplant patients, fragile diabetics and many others whose care plans are predicated on instant telephone support. The practice mentioned above has identified over 200 patients in these categories, and there are severe ethical and legal problems with cutting off their phones – even for 'national security' reasons. It has been argued that the mere threat of a service interruption places the NHS under a legal obligation to admit them all to hospital.

Activating the scheme at the millennium would be more likely to cause panic than calm it: people would assume that the doom-sayers had been right and that this really was The End Of The World As We Know It. The government also doesn't seem to realise that most local loop phone traffic nowadays is fax and data rather than voice. Closing down all phone lines other than those used for voice communications by state sector bigwigs will switch off British business. It would sooner or later cause utility failures: the electricity companies say that their main external Y2K dependency is telecomms. (The University had a more mundane concern: that the system would knock out burglar alarms to about thirty of our buildings. British Telecom reassured us in a letter I got today that burglar alarm service will be unaffected – but we'd already arranged to have extra security staff on duty.)

In short, we are not just at risk of public panic. Governments can also panic, and systems such as GTPS give officials the power to do immense harm by

[2] In theory, the population will be able to dial the emergency services from public telephones, but thanks to competition from mobile phones, these have vanished from many areas

interfering with systems they don't understand. All we can do is hope that the Home Secretary keeps his nerve. If there isn't a national emergency before he presses the red button, there certainly will be one afterwards.

6 Assessment and Conclusions

I can't predict the future. I have written this note because some reduction in uncertainty may be valuable, even as the bell goes for the last lap.

The experience described in this paper indicates that while lots of things may break, few of them will matter much. Many of the concerns we had last year about the millennium bug turned out to be misplaced once we examined the relevant systems in detail. I am now pretty confident that the British government's concerns about small to medium sized businesses are mostly groundless.

There are still risks. The stock market could always crash – but it does this every decade or so regardless of computers. I wouldn't be surprised if we lost a high street business or two, but in most cases this won't matter much: if Superdrug goes bust, you can still buy shampoo from Boots. The failure of a large bank might be more serious, but would still be unlikely to lead to famine. Air transport might be mildly chaotic for a few months, but we can live with that. Some countries may well have left it too late to avoid a certain amount of disruption to utilities; some governments might even fall (dare I say, mostly governments that deserve to anyway). And I expect that there will be some major industrial plant failures; but any which cause casualties on the scale of Bhopal or Chrenobyl are likely to be in places that are less strictly regulated and safety conscious than here. As for the UK, I feel that our main direct risk was public panic. There is still a dangerous bias in the media: the warnings I gave of possible problems back in 1997–8 got massive coverage while journalists consider the reassurance I can now offer to be boring. But boredom may be a good thing. Public boredom with Y2K – especially since the disruption widely predicted for the first of January and the ninth of September 1999 failed to materialise – combined with the generally laid back attitude that people have in these islands, make panic unlikely.

The government is trying to play down the risks, but not in a very convincing way. The line comes across as: 'Nothing can possibly go wrong, and if it does it's the previous government's fault'. This situation is remarkable in that ministers and officials are probably speaking the truth – even though they actually seem to think they're lying. As people distrust government PR anyway, they would probably be better off keeping quiet, regardless of the outcome they expect.

The University's Millennium Committee has had its last meeting; there is nothing left for us to do. As for me, I still have the house in the country, and I'll be spending the Millennium there. The well has broken, and I haven't got round to fixing it. I don't know if I can be bothered.

Coda

A lot of people helped me develop my understanding of the millennium bug problem, but many of them decline to be acknowledged publicly. Some I can credit here, namely Nick Bohm, Caspar Bowden, Robin Guenier, Mary Hawking, Martyn Thomas, and the University staff who are involved in Y2K – including the Y2K Committee and the departmental officers who did most of the legwork, and especially our Treasurer Joanna Womack. Needless to say, the analysis here is my own.

References

1. "The Eternity Service", RJ Anderson, in *Proceedings of Pragocrypt 96* (GC UCMP, ISBN 80-01-01502-5) pp 242–252; available online at `http://www.cl.cam.ac.uk/users/rja14/eternity/eternity.html`
2. "On the Reliability of Electronic Payment Systems", RJ Anderson, SJ Beduidenhoudt, in *IEEE Transactions on Software Engineering* vol 22 no 5 (May 1996) pp 294–301; available online at `http://www.cl.cam.ac.uk/ftp/users/rja14/meters.ps.gz`
3. "Information technology in medical practice: safety and privacy lessons from the United Kingdom", RJ Anderson, in *Medical Journal of Australia* v 170 (15/2/99) pp 181–184; available online at `http://www.cl.cam.ac.uk/users/rja14/austmedjour/austmedjour.html`
4. "Tamper Resistance – a Cautionary Note", RJ Anderson, MG Kuhn, in *The Second USENIX Workshop on Electronic Commerce Proceedings* (Nov 1996) pp 1–11; available online at `http://www.cl.cam.ac.uk/users/rja14/tamper.html`
5. "Rising from the Rubble", G Burton, in *Computer Weekly* (29 Feb 1996) p 20
6. *Private communication*, former BT employee
7. "A Field Study of the Software Design Process for Large Systems", W Curtis, H Krasner, N Iscoe, in *Communications of the ACM* v 31 no 11 (Nov 88) pp 1268–1287
8. 'Y2K Country Statements', at `http://www.fco.gov.uk/`
9. *'Up the creek? — The business perils of computer failure'*, IBM, 1993
10. "Police zapping phones to cope with civil unrest", *Information Security Monitor* v 12 no 9 (Aug 97) p 5
11. "Medical Devices and the Year 2000", Medical Devices Agency, in *Year 2000 and Healthcare Computing*, Health Informatics Journal v 3 no 3/4 (Dec 1997) pp 173–175
12. I Newton, *'Philosophiae Naturalis Principia Mathematica'*, Royal Society, London 1687; reprinted Cambridge University Press, 1972
13. University of Cambridge, `http://www.cam.ac.uk/`
14. "Patient care at risk from millennium bug", J Vowler, *Computer Weekly* (8/5/97) p 3
15. "Business Continuity Planning", K Wong, in *Computer Fraud and Security Bulletin* (April 94) pp 10–16
16. Dr Ed Yardeni's Economics Network, `http://www.yardeni.com/`
17. "Y2K Behaviour Monitor", at *'Online Chart Room'*, `http://www.yardeni.com/`