The Millennium Reckoning
Implications of the Year 2000 computer "timebomb"

Intelligence Update 6.1 - JULY 1999 PREVIEW

INTRODUCTION

Provenance

Trend Monitor has been systematically gathering, analysing and synthesising open source intelligence on the implications of the Year 2000 computer trouble (known as Y2K: Y = Year, 2K = 2000) for nearly four years. Y2K is a small part of a much wider set of subjects -- including the Global Economy - which have been monitored since 1986. The company has used its content analysis techniques on many thousands of articles on Y2K that have been published in the technical, business and daily press, and also analyses the best quality Internet sources.

Process

Trend Monitor's 'information refinery' process extracts key thoughts from its ever growing subject knowledge base and classifies them consistently so that what is being said on a topic at one period of time can be compared with the views and reports on the same topic at other times. The classification process places different views on the same topic into juxtaposition, whereas normally they are scattered at random through the source base. The juxtaposed texts are re-combined and re-told as narrative stories. These overview stories are then used to infer implications.

This process delivers a more holistic understanding of events and also constructs a meta-description of what people are seeing through the "dark glass" of the media. By comparing what is being said at different times, the process makes it possible to see trends in events long before they become apparent even to the most diligent reader. Also, the highly ordered story evidence means that pertinent past events and insights are not forgotten. Trends are then used to underpin and evaluate scenarios, which enable appropriate responses to an ever-changing future of multi-possibilities.

Outputs

Every six months or so for the last three and a half years, Trend Monitor has collected and classified Year 2000 intelligence under four top level categories. 'Perceptions' is about what people think about the problem and is divided into 'Awareness' and 'Risks'. 'Preparations' is about what people are doing and is divided into 'Business', 'Government', 'Costs' and

'Personnel'. 'Problems & Solutions' is about difficulties, as well as strategies, techniques and tools for overcoming the difficulties. 'Effects' is about what is happening as a result of the computer trouble. It subdivides into 'Consequences', 'Lessons' and 'Community Preparations'.

This free Preview edition of the latest intelligence update deals only with 'Perceptions'. The full four-section report will be available at the end of July 1999, along with fully updated 'Trends' and 'Scenarios' sections. The price, which includes monthly Updates in September, October and November is £300 for companies and governments and £125 for voluntary organisations and businesses with less than 10 employees. For individuals the full July 1999 Update costs £25.

For further information please contact: sales@trendmonitor.com

To see Trend Monitor's full intelligence collection on Y2K please visit our website at http://www.trendmonitor.com/

Trend Monitor
"The Information Refinery"
3 Tower Street
Portsmouth
Hampshire
PO1 2JR
UK
Tel: +44 (0)1363 881017 or +44 (0)1705 864714
Email: jan@trendmonitor.com
Web: http://www.trendmonitor.com/

PERCEPTIONS

Awareness / Ignorance

Implications

After more than three years of constant but fragmented media reporting, most people still fail to understand the reality of the risks that Y2K presents. The real tragedy of this lack of understanding is that it prevents people from taking appropriate contingency actions. A process of denial leading to action that is too late has been the case all along, first by computer professionals, then by their managers and now by the government and the public. It is the principal reason why the risks are now so great.

Stories

An article by Karl Feilder in *Computer Weekly* on June 17, 1999 says: "Two of the largest software companies in the world recently told me that they have given up trying to persuade the average PC user that the Year 2000 problem is more than a BIOS issue." The article also makes the point that "Other companies trying to help in the Y2K arena all report the same

thing - interest has dwindled. This despite the fact that we have only just touched the tip of the iceberg."[1] In an article he wrote for *Computer Weekly* in April 1999, Mr. Feilder characterised the vast majority of computer users as having no knowledge or interest beyond their own narrow application. This attitude, he thinks, explains such widespread ignorance about the millennium bug.[2] Another reason why people are ignorant about the computer trouble is that governments and companies are thought to be withholding information for reasons such as commercial confidentiality or the avoidance of panic.[3] [4]

Communications International reported in February 1999 that "senior managers have been slow to grasp the seriousness of the Year 2000 problem because the socio-business etiquette makes it hard for the relevant subordinates to tell them about it". The article goes on to say that "In China, the head in the sand attitude has been reinforced by the fact that, for them, the year begins at a different time. But unfortunately for China, western time is the global standard for computers."[5]

References

1. Are US bug projects slipping into the darkside? - *Computer Weekly*, June 17, 1999
2. It all comes down to whether Ethel can do her job - *Computer Weekly*, April 22, 1999
3. The writing on the wall for IT: are we headed for a global crisis? - *Business Week*, March 22, 1999
4. Air industry will not name millennium danger spots - *Independent*, May 4, 1999
5. Time stands still ... - *Communications International*, February 1999

Awareness / Knowledge

Implications

The vast majority of adults, whether they are educated or not, are not trained to think either holistically or in terms of systems. Instead people are taught to think in fragmented and compartmentalised ways. Narrowly focused, expert knowledge has been valued much more highly than whole systems thinking. Quantative statistical measures are considered more valid than qualitative insights. The Year 2000 trouble is very much about how huge systems -- e.g. energy and transportation -- will influence each other. Linear statistical measuring techniques, such as the percentage of the job completed, are virtually meaningless when so many influences and uncertainties need to be considered. Since the interactions within and between systems is so great, a basic understanding of Complexity thinking is also crucial. These kinds of factors are seldom considered because they are outside most people's expertise. Yet, it is precisely these questions which are at the heart of the Y2K trouble. People simply don't know how to ask the best questions.

Stories

Writing in *The Independent*, Sophie Radice describes her eight year old son's understanding of the Millennium Bug: "Do you realise that all the traffic lights will stop, so all the cars will

crash into each other, and the hospitals won't even work any more. There will be no electricity or heating supplies or water, so everything will be cold and dark, so there will be no food. There will be nothing left, Mum, can you understand that?" The article concludes, "primary school children do seem to have a deeper understanding of just how much our society is controlled by computers and just how much we all rely on them".[1]

Another consideration is profound uncertainty. In the words of Andrew Charlesworth writing in *IT Week*, "Even if you think your systems are OK, no one really knows what the knock on effects will be of others who are just as sure as you."[2]

References

1. Millennium bug bites children hardest - *Independent*, March 22, 1999
2. You just don't know - *IT Week*, March 29, 1999

Risks / Environment

Implications

The threat to the environment posed by rollover failures in date sensitive microchips has received little media coverage. It is reported that problems with these "embedded systems", which act as control or monitoring mechanisms in a wide range of plant and machinery, could lead to malfunctions in water purification plants, sewage systems, oil refineries, pipelines, off-shore platforms and supertankers, chemical plants, nuclear and coal fired power stations, hazardous waste facilities, and weapons systems. Experts are said to vary in their estimations of the failure rate in embedded systems, though most agree that only a very small percentage are liable to cause safety problems. However, concerns have been expressed about the "domino effect" of failures in highly interconnected and interdependent systems. Some experts are predicting a global scenario in which several major disasters of the magnitude of a Bhopal, Exxon Valdez or Chernobyl occur almost simultaneously, placing an unprecedented load on the resources of emergency response units. With many scientists reported to be deeply concerned by global warming, species loss and the deteriorating state of the environment, there are fears that a worst case Y2K scenario could tip the scales of ecological balance and threaten nature's ability to continue providing the essentials of human survival -- food and water. In the northern hemisphere a harsh winter would compound the systemic problems that may arise from Y2K failures. The vulnerabilities that Y2K is exposing may lead to a deeper appreciation of the need for a more sustainable, ecologically sound and less technologically dependent basis for our societies.

Stories

Dr. Paula Gordon of George Washington University has said, "In our highly specialised world, relatively few people even know about the existence of date sensitive embedded systems. Of those who do, fewer still understand the complex technology. Very few public officials in any branch or at any level of government have readily grasped the significance

that date sensitive embedded systems have in the context of the Year 2000 technology crisis."[1]

On May 5, 1999, in an article titled "2000 bug threatens pollution disaster", the *Guardian* quoted an Environment Agency report which said "There is the potential for bug-related systems failures to cause severe damage to ecosystems and rivers, releases of noxious fumes and effects on drinking water supplies."[2] The report said: "Results of a recent survey by the Environment Agency show that the millennium bug poses a serious threat to the environment and has the potential to cause environmental damage unless companies take preventative action now. More than half of the companies surveyed still have significant amounts of work to do." The report continued: "Many environmental management and protection systems are controlled by computers and include microprocessors. A pollution event may happen if the bug disrupts systems and leads to uncontrolled releases of harmful substances."[3]

In January, Y2KNewswire.com issued a statement "urg(ing) municipalities to cease water flouridation during Y2K rollover to avoid risk of fatalities." The article noted that "Over the last 25 years fatalities have occurred when fluoride saturation levels ran too high, some due to faulty flow control systems." It quoted a story related by Senator Robert Bennett that was reported in the *Salt Lake Tribune* on January 18, 1999. "Curious about what would happen when the new millennium ticks in, a water purification plant in Utah set its clocks ahead to Jan. 1, 2000. With computers ill-equipped to handle the new date, the plant malfunctioned, dumping poisonous quantities of chlorine and other chemicals into the water."[4]

References

1. A call to action: the national and global implications of the Year 2000 embedded systems crisis - http://www.gwu.edu/~y2k/keypeople/gordon/
2. 2000 bug theatens pollution disaster - *The Guardian*, May 5, 1999
3. Pollution threat from the millennium bug - Environment Agency Report, May 1999
4. Y2KNewswire.com urges municipalities to cease water flouridation during Y2K rollover to avoid risk of fatalities - January 21, 1999 http://www.y2knewswire.com/

Risks / Energy

Implications

If the Russian natural gas pipeline supplying both Eastern and Western Europe is interrupted, as Russian experts say it almost certainly will be, it will be very difficult to start the gas flowing again with an uncertain electricity supply and sub-zero temperatures. Oil stops flowing at freezing temperatures which means that pipelines and refineries are at risk, even if there are relatively short power outages. In the US, which is far ahead of Russia in its preparations for the energy sector, major oil companies are reportedly adopting a fix on fail (FOF) policy on wells, pipelines and refineries.

Another reported implication is that if the electricity fails, some nuclear plants may have

difficulty cooling their cores if they are to be shut down, creating a real danger of accidental melt-downs.

The economic, environmental and social implications of the failure of the Russian gas and oil pipeline network are so enormous -- for Europe and the rest of the world -- that the necessary resources must be made available on an international level to ensure that:

i. the operation of the Siberian gas pipeline network is made secure;
ii. nuclear reactors everywhere have sustainable back up electrical systems which do not depend on national grids;
iii. as many alternative local electricity sources are built as possible.

All the countries and people of Europe are at risk of having to deal with the consequences of severe energy shortages and consequent energy price increases.

Although it is by no means certain that this worrying scenario will come true, even if no remedial action is taken, the seriousness of the multiple risks warrants emergency action now on a "just in case" basis. A huge investment in sustainable energy systems is required, both for deployment around nuclear sites and within communities. The task could be do-able in the time remaining if an international crash programme were to be implemented in the next few weeks. It is a question of mobilising people and money to secure the future very quickly. Not only would the short-term problem be solved, the implementation of an economical long term solution could be accomplished at the same time.

Continuing denial by governments and the media of the possible magnitude of the risk to key energy systems is the greatest danger at the moment because it is preventing people and companies from making appropriate contingency preparations.

Stories

An April 1999 article in *Computer Business Review* quotes Professor Andrey Terekhov, a Russian Y2K expert, as saying "the gas and electricity started work so late that their systems simply will not be ready in time". The article concludes that this news has "ominous implications", not just for Russia, "but also for the countries in Europe which are dependent on Russian gas".[1]

In March 1999, UK energy companies were seen as well prepared, according both to their own spokesmen and to Action 2000's National Infrastructure Status Report.[2] However, in June 1999, the *Financial Times* reported that the energy industry was still "spending heavily to ensure that their complex computer systems suffer no ill effects" from the millennium change over. The article warns that "anticipation of chaos" is liable to push up the price of oil as the end of the year approaches. The article also questions the well publicised confidence of the energy sector, citing Chevron which said "it could not tell whether it would suffer significant business interruptions, including the shut down of its entire oil and gas production", although the company expected disruptions to be "localised". [3]

Sources within the US oil industry are quoted in an editorial appearing on the Golden Eagle website saying: "Overall, these sources estimate that based on prior limited testing, they are

expecting a 10 to 20% ratio of failure, or multiple embedded systems going down on each oil well. There will be no parts to fix them and no replacement systems available for quite a long while. These sources tell me that the major oil companies have adopted a FOF (fix on fail) policy, because it is the only affordable and practical approach."

"The bottom line: most oil well embedded systems were never, and are never going to be checked or tested for Y2K compliance. Its a virtual impossibility...And even if they did, most likely the parts to replace them will no longer be available. It's now become very difficult to find anyone who can supply a replacement system before 1/1/2000. Some easier testing was done on more accessible systems, which are usually newer. Understandably, fail rates have soared 25% in some areas."

On the subject of oil and gas pipelines, the author says, "The same that was said about the well heads and embedded systems is true for the pipelines. It's just too complicated -- and the major companies decided to adopt the FOF policy -- and wait to see what breaks down and to subsequently try to fix it. Another consideration is loss of electricity for any significant length of time."

The other point made in the article is that the oil industry -- like so many others -- works on the basis of a "just in time" supply principle. Consequently stocks of oil and natural gas are very low.[4]

Although there is little reported in the UK newspaper and magazine source base on the risks of nuclear energy plants, Reuters reported from the US on June 18, 1999 in an article entitled "US proposes stock piling radiation antidote", that the Nuclear Regulatory Commission (NRC) had proposed the stockpiling of potassium iodide, which helps "prevent radioactive iodine from being lodged in the thyroid gland, where it could lead to thyroid cancer or other illness".[5]

In an article entitled, "The Accidental Armageddon", Helen Caldicott, an anti-nuclear energy campaigner, warns that the circulation of coolant water is "dependent on an external electricity supply and an intact telecommunications system. If the millennium bug causes power failures and/or telecommunication malfunctions, reactors will be vulnerable. Because of this possibility, each US reactor has been equipped with two back-up diesel generators. But at best these are only 85 per cent reliable. So, in the event of a prolonged power failure, the back-up diesel generators will not necessarily prevent a nuclear catastrophe. And 67 Russian-built reactors are even more vulnerable, because they have no back-up generators.

"What is more, the Russian electricity grid is itself at great risk because, as one might expect, the political and economic turmoil in that country means the Y2K problem has hardly been examined. There are 70 old nuclear reactors on old Russian submarines moored at dock in the Barents Sea. If they were to lose the electricity grid powering their cooling systems, they would melt."

The article advocates a crash program to provide all the world's nuclear reactors with wind and solar electricity generators to insure that enough electricity is always available for the cooling necessary to prevent meltdowns.[6]

An article in the *Independent* on July 4, 1999 cites an internal memo circulated in the British Embassy in Moscow which says that Russia is "one of the countries most vulnerable to Y2K problems". Among the concerns listed in the article is the provision of "back up generators for nuclear power stations."[**7**]

"Midnight Crossing" published in the July 1999 issue of the US *Airforce Magazine*, says: "US officials are very concerned that a computer failure in Russia's interconnected power grid could cascade through the entire nuclear system and lead to a massive power outage. Such an event could easily end in catastrophe at one of the 65 Soviet-made nuclear reactors." Human error by "an undermanned and unmotivated" (and often unpaid) nuclear work force is increasing "the possibility that a power outage at a nuclear reactor could lead to a catastrophe". Even if the nuclear reactors are managed well, the article says, "loss of power and cooling at the numerous waste pools where atomic fuel rods are kept could cause the water to boil away and permit the release, into the local atmosphere, of lethal levels of radioactivity. Recently loaded rods -- those placed in the waste pools within the past two years -- could begin to melt down within 48 hours of a loss of power".[**8**]

According to a database called "Diesel Generator Defects at US Nuclear Plants" compiled by the US Nuclear Regulatory Commission, reports from January 1, 1999 to the present "show that defects and problems occur on a weekly basis in the US nuclear power industry. There are 27 reports affecting 41 plants; or 40% of all US commercial nuclear plants so far this year." Scott D. Portzline of Three Mile Island Alert comments in " The Weakest Link: Emergency Diesel Generators (EDGs) " that during a "station blackout" (loss of offsite power) these generators "supply the electricity needed to bring the plant to a safe shutdown". If they fail, it is said that the chance of an accident "approaches certainty". Former NRC Chairman Dr. Shirley Jackson is also quoted saying, "NRC reviews in recent years have left no doubt that a station blackout at a nuclear power station is a major contributor to reactor core damage frequency." Although the NRC is reported to be claiming a 97.5 per cent reliability, "watchdogs say it is lower".[**9**]

References

1. **1.** Russian bug threatens cold winter of discontent - *Computer Business Review*, April 1999
2. **2.** Questions linger on energy - *Financial Times*, March 3, 1999
3. **3.** Industry tries to avoid hazardous flare-ups - *Financial Times*, June 22, 1999
4. **4.** Oil and natural gas: are they the real problems in Y2K? - June 21, 1999 http://www.gold-eagle.com/editorials_99/rc062199.html
5. **5.** US proposes stockpiling radiation antidote, by Tom Doggett - *Reuters* Washington, June 18, 1999
6. **6.** The accidental armageddon - *The Age* (Australia), June 20, 1999 http://www.theage.com.au/daily/990620/news/news22.html
7. **7.** Diplomats warned off Y2K Russia - *Independent*, July 4, 1999
8. **8.** Midnight crossing - *Airforce Magazine*, July 1999
9. **9.** Emergency Diesel Generators: The Weakest Link - Three Mile Island Alert, July 1999, http://www.tmia.com/EDGs.html

Risks / Transport

Implications

The bottom line with 20th century transportation systems is that nothing moves without fuel ... including food. If the oil and gas system is under serious threat, as the Energy stories suggest, so is the whole transport system. Suddenly, the name of the game becomes fuel rationing and the maximisation of local self-sufficiency. Under these conditions, global trade would contract and the cashflow of global corporations would decrease sharply. How many big energy and transport companies could go bankrupt? On the otherhand, the smart money would go towards investing in local sustainability. If the nuclear meltdown threat can be contained, then there is a potential for smart investors to make fortunes by investing in local food production, local businesses and local community services.

Stories

In February 1999 Tom Brown, responsible for "bug busting" at the US Air Transport Association, said: "Airplanes aren't going to fall out of the sky - the issue is whether they will take off. Are we going to have fuel? Are we going to have runway lights? Are we going to have fire trucks?"[1] Even at that time airlines were reported to be releasing prices for travel in December 1999 at "steeply increased rates".[2] According to *The Independent* on July 1, 1999, a study by the British Airline Pilots' Association found "serious shortcomings in most countries' preparation, especially those in the developing world" and said that "Air travel from Britain to many parts of the world will be virtually impossible over the new year because of fears about the Millennium Bug".[3]

According to a confidential source in the shipping re-insurance industry, the Year 2000 challenge has created "unprecedented co-operation" amongst both big and small shipping groups. The work done so far, he said, has been "competent and well focussed". As for shippers obtaining coverage against Y2K-related losses, "the more you do the more likely you are to be covered". However, he did quote the manager of one of the world's best prepared ports which had already fixed and tested all the computer problems and embedded chips they could find, who said it was impossible to be sure whether the whole port system would work on the day because "you simply can't reboot the port."[4] A further complication in sea transport is that the administration of the Panama Canal is being transferred from the US to Panama at mid-day on December 31, 1999. The acting Chairman of the Canal Board is quoted as saying: "Since we operate ships in confined spaces, we are concerned about the potential problems this might represent to the canal".[5]

UK and US rail organisations say that they are "on track" towards providing normal services over the millennium period. However, a June 11, 1999 report in the *Philadelphia Inquirer* about the US rail company takeover of Norfolk Southern by CSX, notes the ease with which chaos and gridlock can overtake a rail system. The article quotes a major shipper, who asked not to be named, who noted that the massive service meltdown that crippled western shipping after the 1996 Union Pacific takeover of Southern Pacific "didn't happen overnight." That debacle "built up incrementally until there was gridlock", the shipper said.

Gary Galvin, an official of the United Transportation Union, which represents conductors and brakemen aboard trains, said he is hearing reports of huge crew-management and computer problems on Norfolk Southern. High-priority cars are going around the system "hundreds and hundreds of miles" out of their way, he said. Employees trying to report problems have not been able to get through on the phone numbers they are supposed to call. Galvin said Norfolk Southern is cutting its local managers out of the decision-making."[6]

References

1. Hoping to avoid disruption - *London Times*, February 27, 1999
2. Bug that threatens chaos in the air - *London Times*, February 27, 1999
3. British pilots threaten millennium flight ban - *Independent*, July 1, 1999
4. Confidential - June 30, 1999
5. Year 2000 alert for shipping - *Financial Times*, April 14, 1999
6. Shipping snags develop as Conrail split takes hold - *Philadelphia Inquirer*, June 11, 1999

Risks / Communications

Implications

These days most financial transactions take place over the global telephone network. What will happen to the hundreds of billions being traded around the world every day if telephone networks in countries such as China and Japan are prone to disconnection? The telecommunications difficulties are liable to make international trade very much more difficult and expensive. Physical distance would again become a factor in trade. Under these conditions, local self-sufficiency would become increasingly advantageous. If energy supplies are interrupted, then postal services will also be liable to breakdown. For the duration of the chaos, the ability to trade over long distances may be lost altogether.

Stories

According to *Communications International* in February 1999, as a result of a slow start in Y2K projects "it now looks like many telcos in the developing world, and some developed carriers in East Asia will not have compliant systems by 2000, and the result could be that calls made to subscribers will fail and not be terminated."[1] According to a Foreign Office survey in March 1999, computer breakdowns in "middle ranking" nations will hit telecommunications.[2]

In February 1999, *Computer Weekly* reports telephone equipment suppliers "accusing" businesses of Year 2000 apathy by "ignoring the problem or delaying repair work". Suppliers are said to be "bracing themselves for a last minute rush of fixes and upgrades, but warn that they may not have the resources to deal with demand".[3]

The March 1, 1999 edition of *IT Week* maintained that "if the software in a GPS (Global

Positioning Satellite) receiver is not corrected, then the receiver will internally interpret the new week zero as 6 January, 1980, stopping its capability of tracking satellites as it loses synchronisation", thereby threatening air and sea navigation systems.[4]

References

1. Time stands still - *Communications International*, February 1999
2. Nations face millennium bug blacklist - *The Independent*, March 19, 1999
3. Firms slam users' Y2K apathy - *Computer Weekly*, February 18, 1999
4. Millennium may arrive early - *IT Week*, March 1, 1999

Risks / Financial services

Implications

Just as you can't "reboot a port", you can't reboot the globalised financial system. Nobody can be certain whether Y2K will turn out to be a blip, a collapse, or something in between. The public perception of what will happen will be a determining factor. Another factor is whether survival businesses -- such as local renewable energy systems and bulk food purchasing and supply -- will be in a position to gear up fast enough to be able to take the huge amount of investment potential from money seeking a "safer haven" than the highly exposed global corporations and banks which now dominate investment portfolios. It is even possible that bank money will lose its value, while cash becomes the main medium of exchange, therefore retaining its value. Under these conditions, local community currencies would become a useful tool for keeping the local economic wheels turning.

Stories

An article in the *Times* on March 20, 1999 stated that: "The international nature of the financial services industry does exaggerate the risks that it faces, for much of the rest of the world certainly has lagged behind the UK in year 2000 preparations." The article reports "widespread scepticism" in the City of London about the ability of European financial institutions to meet the deadline. It also makes the point that even if technically it has more deposits than loans, "any bank that stops trading, even for a matter of days, becomes insolvent". The question arises of what happens to banks that are trading with financial institutions whose assets have been frozen? The article says that "this systemic risk" is "the spectre that haunts financial regulators." The possibility of people withdrawing all their cash from the bank is characterised as not being "quite so misguided" on the basis that "the financial industry is like a house of cards". The article reports, for example, that "At a high powered meeting in Washington recently, delegates were stunned to hear Henry Kissinger announce that he intended to withdraw all his money from the bank as 2000 nears".[1]

According to the Bank for International Settlements (BIS), the greatest concern of the banking industry is "the possibility that access to wholesale funds could be affected by failures in payment and settlement systems". Already in February 1999, the BIS had pointed

to "a sharp increase in the cost of funds towards the end of this year, suggesting that investors are anticipating a liquidity squeeze".[2]

In February 1999, the UK Financial Services Authority (FSA), announced that 12 of the most important financial institutions in the UK were in "serious danger", while "a further 56 big firms were behind schedule but likely to get on track".[3] According to Robin Guenier, the executive director of Taskforce 2000, the FSA also said that "none of Britain's top 500 financial institutions was yet ready for the date change, even though every major financial business business I spoke to in 1996 said the job had to be done before the end of 1998". Mr Guenier asks rhetorically: "How often does a computer project that's fallen behind catch up?" His answer: "Very rarely." [4] At the end of June 1999, the FSA reported that only one financial institution was classified as Red -- "at serious risk of seeing its business materially disrupted". According to the *Financial Times*, this unnamed institution had previously been classified as Amber -- "behind in its preparations but likely to get on track". It is also reported that the FSA is planning to require all senior executives of financial institutions "to notify the regulator when they had completed their year 2000 programmes".[5]

References

1. Headaches start as the bug bears down on banks - *The Times*, March 20, 1999
2. BIS puts world's banks on 2000 bug alert - *Independent*, February 27, 1999
3. Financial giants fail on 2000 bug - *Independent*, March 18, 1999
4. Bug that threatens to topple the world - *Observer*, April 11, 1999
5. Millennium bug risk 'still threatens one City body' - *Financial Times*, June 16, 1999

Risks / Public services

Implications

In addition to food, water and drug distribution, the bottom line for health services anywhere in the world is the maintenance of energy, transport and communications systems. In a sense, hospital computer systems are no longer the most important issue. Hospitals and other public services are now faced with the question of whether stockpiling basic provisions, including fuel for generators, is the prudent choice given the risks in the supply chain. Companies are already stockpiling. The care of the infirm in their homes under these kind of conditions necessitates the mobilisation of local voluntary groups.

Stories

The UK National Health Service continues to be the focus of stories about new risks. In April 1999, *Computer Weekly* reported that "The health service is concerned that while hospitals, GPs and other groups are pressing ahead with their own in-house Year 2000 programmes, they could be overlooking patients who use potentially date sensitive medical equipment at home." The options which the NHS is "considering" are listed as: "**1)** raising awareness among community nurses and outpatient departments, **2)** providing information

through GPs' surgeries, and **3)** making information available through Action 2000."[1]

In May 1999, the National Audit Office is reported to have "identified problems with ensuring the supply chain of goods and services was working efficiently". [**2**] *The Independent* of June 18, 1999 reported that "Ministers admitted yesterday that they could not "guarantee" the millennium bug would not cause disruption to public services, as new figures showed Whitehall departments behind schedule in tackling the problem." It is estimated that 20 per cent of government departments were "still not ready" for the date change with the Ministry of Defence, the Inland Revenue and National Insurance Contributions Office selected for admonishment by Margaret Beckett, the Minister in charge.[**3**]

References

1. NHS fears Y2K will hit home-based equipment - *Computer Weekly*, April 15, 1999
2. Millennium danger at one in 10 hospitals - *Independent*, May 5, 1999
3. 'No guarantee' on bug problem - *Independent*, June 18, 1999

Risks / Computer systems

Implications

The potential for hoaxes, virus attacks and theft will be at an all time high, not just for a week or two before and after the New Year, but for a much longer period of time. This new insecurity is something that business will have to face -- both internally and externally -- at the same time as they begin to experience the consequences of the millennium bug itself. Microsoft has ensured that in the realm of PC networks, date confusion will continue well into the next century.

Stories

In addition to the well known threat of date confusion, a new fear is reported in *Computer Weekly*, which warned on June 17, 1999 that "A new generation of viruses that cause havoc by re-setting the central clocks of mainframes and PCs could strike before the end of the year". The article refers to "rising concern" among IT managers that criminals, terrorists or disgruntled staff "could exploit the millennium bug as cover for hacking and virus attacks". Martyn Emery, director of Year 2000 consulting firm Corporation 2000, is quoted as saying "Companies could be hit by thousands of viruses ... It may be that companies will have to disable their email systems for the first seven days of the new year".[**1**] An article in *The Independent* quotes the Bank of International Settlements saying: "Particular attention should be paid to the increased possibility for fraudulent attacks on information and accounting systems at times of system disruption".[**2**]

Microsoft's introduction of Windows 2000 and Office 2000 is regarded as another new risk. In addition to the inevitable complications involved with upgrading operating systems, a new date window function enables users to enter two digit year dates "and have the computer

automatically guess the century". According to Karl Feilder writing in *Computer Weekly*, "The end result is that any input or output of data depends on whose PC is using it".[**3**] On June 3, 1999, Microsoft president Steve Ballmer warned that "businesses must expect a period of chaos following the roll out of Office 2000 which allows end users to participate in knowledge management".[**4**]

References

1. Hackers use Y2K bug as a smokescreen - *Computer Weekly*, June 17, 1999
2. BIS puts world's banks on 2000 bug alert - *Independent*, February 27, 1999
3. Microsoft's gift-wrapped machine gun - *Computer Weekly*, July 1, 1999
4. Microsoft president voices Office 2000 chaos theory - *Computer Weekly*, June 3, 1999

Risks / Economy

Implications

It seems that the threat to the economy is not from either big companies or small companies, but from both. New companies and very small companies that can become date compliant in a matter of minutes would seem to have the economic advantage in a post-Y2K world. The market in unsold stock and assets from bankrupt companies is likely to grow very quickly too. The economy would be reminiscent of the barter markets in post-Soviet Russia. But unlike the experience in Russia to date, barter currencies would likely be used to enable the smooth, cheap and easy operation of a generalised barter market. Will the banks, which underpin the global economy, survive? In all likelihood, some will and some won't. There would be hard currencies, but they are liable to be too scarce, unstable and uncertain in value to be much use. The potential growth of the barter market, where knowledge and skills as well as goods are traded, is likely to be very significant. Transport expenses in a post-Y2K economy are likely to be very high, while volume of trade would be very low which could mean potentially very high profits for the shipping companies that survive. The oil and gas industry might also do rather well from sharp price rises if they can maintain supply. Air transport will be hit doubly hard by rising fuel costs and falling passenger and freight demand.

It must also be noted that the potential economic turmoil brought on by Y2K will hit the global economy at about the same time that the US asset and credit bubble is liable to burst. The combination of these two forces really could mean the end of the global economy as we know it, as the world fragments into a complex of local economies.

Stories

At the end of January 1999, *IT Week* identified conflicting claims between the UK's independently funded Taskforce 2000 and the government agency Action 2000. "The Taskforce 2000 research shows that large companies are alarmingly behind in their Year 2000 preparations, while Action 2000 says large companies are on schedule and the real

threat to the economy is the supply chain."[1] According to *Business Week* on May 10, 1999, 69 per cent of US companies are freezing computer development, a condition called "lock down" because they have "fallen behind their Y2K testing deadlines or are running into unexpected glitches". The article quotes Allan Graham, the vice president of Comdisco Inc., a company which tests Y2K repairs: "The Year 2000 problem is like an onion, every layer you peel off the more you want to cry. You find there are deeper problems."[2] On July 1, 1999, *Computer Weekly* reports a study by Taskforce 2000 and London law firm Dibb Lupton Alsop, which suggests that one third of the UK's top 1000 companies admit to being behind in their Y2K work.[3]

On June 19, 1999, *The Guardian* cited a study of 500 companies by the Cranfield School of Management which suggested that "at least 60 per cent are stockpiling raw materials and finished goods because of fears the bug will interrupt the supply chain next year". The study is also said to have found that "the bug presents a threat to developing countries as companies switch to suppliers in countries more likely to have prepared for the problem".[4] [5] Industries that are expected to be especially hard hit next year are the computer industry (as a consequence of "lock down") and industries that cannot stockpile, such as airlines.[2] [6] According to an article in *Business Week*, some bank stocks, such as CitiGroup, are liable to "plummet some 40 per cent during the fourth quarter of this year and the first quarter of next year". The main reason is said to be "international exposure to third-party entities that are "Y2K-unprepared".[7] Another risk put forward in the *Financial Times* on June 7, 1999 is that if trading "slows to a trickle" in the last few weeks of the year, it will create a "thin" and "volatile" market in which a "sudden downturn in prices might be wrongly interpreted as panic".[8]

References

1. Order from chaos - *IT Week*, January 15, 1999
2. This Y2K bug is already loose - *Business Week*, May 10,1999
3. Top firms on Y2K danger list - *Computer Weekly*, July 1, 1999
4. Stockpiling fear as millennium looms - *Guardian*, June 19, 1999
5. Could the bug bite the world economy - *Sunday Times*, March 21,1999
6. We are all bitten by this bug, like it or not - *Independent*, March 31, 1999
7. The sky isn't falling - *Business Week*, June 14, 1999
8. Millennium bug - *Financial Times*, June 7, 1999

Risks / Countries

Implications

In an integrated global economy, there is no way that relatively well-prepared countries can avoid the consequences of the vast majority of countries being woefully ill-prepared. Commercial supply chains, which are dependent on components from the Far East, will almost certainly be interrupted. Banks and corporations with investments in the Far East, South America and the Third World are almost certain to experience defaults on payments

and frozen accounts, which will threaten their solvency. Companies with the least international exposure will be in the best position, which means that the Far East, the Third World, Russia and Eastern and Continental Europe will suffer a process of disinvestment at the very time that they need the most investment in Y2K remediation and contingency planning. National governments will have to turn quickly towards doing everything possible to stimulate local sustainability, rather than global competitiveness. All it takes is a change of mind and a change of policy, which will be almost inevitable if Y2K destroys globalisation within a matter of months. It becomes a question of which governments break ranks first and when. If it comes to de-industrialisation, Third World countries, Eastern Europe and Russia will have the advantage over more developed countries because their populations know how to grow food for themselves.

Stories

Although there is disagreement among experts on the state of preparedness of countries such as the US, Canada, the UK, Scandinavia and Australia, there is universal agreement that virtually all of the rest of the world is dangerously unprepared. In the words of *The Observer*, "most mainland European countries, the far East and almost all Third World Countries are far behind in their preparations, and chaos could have knock on effects in Britain and the US."[1]

Writing in *Computer Weekly* in May 1999, Karl Feilder compared the attitude of people just waking up to Y2K in Europe to that of 50 African ministers who met and "admitted that they had thus far done nothing about the Year 2000 problem". He expressed this attitude as, "Please help us -- we are too late to sort this out on our own, so won't you ... show us how to do it." His response to them is: "There will be no magic solution -- no miracle aid from overseas -- you must rise to your own challenge."[2] In another article Mr. Feilder answers the question of how mainland Europe is doing, saying "not well on the whole and very late, with the Germans still struggling to believe that this is really happening".[3] A May 31, 1999 article in The *Financial Times* reported that European Union officials "expressed concern" about the readiness of Italy, Greece and Spain. France and Germany are said to have "embarked late on preparing for the problem, but were making progress".[4]

Russia is seen as "suffering political and economic upheaval, which had hampered preparations". The accent in Russia is said to be planning for contingencies "if things break down, rather than making computers Year 2000 compliant". A *Financial Times* report in March 1999 says that Russia was attempting "to play down the threat posed by the millennium computer bomb to its military installations, while saying it had earmarked less than $4 million to tackle the problem". NATO sources are cited saying, "Our assessment is that Russia is way behind the curve".[4] [5]

At the end of March 1999, Gartner Group research suggested that "Japan's Year 2000 readiness had moved into line with other industrialised nations". However, the *Financial Times* reported that investors and analysts "remain sceptical" because the government's "battery of statistics" had been "laundered" and few companies had "disclosed Year 2000 related efforts or spending". Japan's problems were said to have been "compounded" by its "complicated Web of cross shareholding" which makes it difficult to "anticipate the domino effect of a glitch at any given company". Yet another concern was said to be companies'

general lack of resources to handle the Year 2000 problem, "with the shortage acute in small and medium enterprises".[6] In March 1999, the *Financial Times* warned that deregulation is "hampering preparations for Year 2000", while "many banks and brokers are, in addition, financially weak and have been slow to address the potential for disastrous computer malfunctions."[7]

On June 14, 1999, *The Independent* said that "Japan's failure to prepare adequately for the millennium bug is posing a threat to the troubled Japanese economy and has grave implications for manufacturing exports around the world." The article said that although leading manufacturers, such as Sony and Mitsubishi, are "likely to have completed their preparations in time", the trouble is with "smaller companies and subcontractors, which make up 80 per cent of Japan's manufacturing industry". The article also makes the point that Japan supplies a large portion of components for manufacturing, especially for high tech industries such as the US computer industry.[8]

A Gartner Group report at the end of March 1999 was quoted in the *Financial Times*, saying "Efforts to get less-developed countries and lagging industries moving more quickly have met with minimal success by international groups and associations." The report listed the sectors which were "furthest behind" as being "airports, shipping and railroads, health care, agriculture, construction and education.[9] At the end of June 1999, the *Financial Times* reported a UN warning that "many developing countries face severe trade disruption and loss of vital tariff revenues ... because their computerised customs systems cannot cope with the Year 2000 problem." UNCTAD was reported to be trying to raise $11 million to fund procurement of new hardware and operating systems for the 60 or so companies requiring it.[10]

References

1. Millennium bug-busters say the panic's all over - *Observer*, March 14, 1999
2. Major act of heroism needed for Italian job - *Computer Weekly*, May 3, 1999
3. Attitudes change as the awful truth dawns - *Computer Weekly*, April 8, 1999
4. N Europe prepared for Y2K - *Financial Times*, May 31, 1999
5. Russia plays down dangers - *Financial Times*, March 3, 1999
6. Year 2000 problem likely to strike nine months early - *Financial Times*, March 31, 1999
7. Year 2000 fears spark Western worries over Japan - *Financial Times*, March 17, 1999
8. Japan faces computer chaos - *Independent*, June 14, 1999
9. Gap wider over Year 2000 - *Financial Times*, March 25, 1999
10. Developing countries 'face Y2K trade problems' - *Financial Times*, June 25, 1999

Risks / Society

Implications

Low mainstream coverage in this category suggests that insufficient thought is being given to the social risks of Y2K. One article cited was clearly written to shock...the horror of people starving in the midst of anarchy and civil war is too much for most of us to bear. Still,

it happens all over the world, with Kosovo being only the most recent example. Some reports suggest that the best antidote to this scenario is local community co-operation and self-help. But in an individualist society, will it be "every man for himself", or can we regain the community spirit that many of us have lost? Although the "panic factor" -- the way that people respond to this crisis -- is thought by some to have as much potential for causing chaos as the computer trouble itself, this contradicts a Red Cross study of 300 disasters. According to proponents of community preparation, it is up to us whether we co-operate or compete over scarce resources. The fact that the cause of the crisis is an abstract electronic computer code rather than a specific person or group may help to bring out the best in people, unlike most cases of social breakdown where scapegoating has often played a major role.

Stories

Organizational Development expert Margaret Wheatley said in an article published on the Internet in May 1999 that "What began as a simple "technology problem" has mushroomed into a problem that has the potential to disrupt every major system -- economic and social -- that we have created."[1] An article in *GQ* magazine titled "System error: welcome to the last year of your life" outlines what it calls the "blackout scenario". This kicks in "if there is less than 70 per cent success rate in making the world's computers Y2K compliant". This scenario portrays "hundreds of thousands of starving people" while helpless and powerless governments look on.[2] A special issue of *Wired* magazine in April 1999 compared a worst case Y2K scenario with the dislocation caused by the Montreal ice storm of January 1998 and the 5 week power outage in Auckland from February-April 1998. It said, "If the ice storm in its immensity resembled a hurricane, the Auckland outage was a tornado: It picked up most of the 76,000 office workers and residents of Auckland's central business district and put them down somewhere else...Suddenly Auckland was being compared to...a third world city."[3]

A *Sunday Times* article in January 1999 suggested that "If stockpiling and the building of survivalist retreats move beyond the concerns of a few and into the mainstream, the effects could be devastating, bug or no bug."[4] Also in January 1999, *Vanity Fair* carried an article which reported that "A recent survey of technology executives found that 10% of them planned to stockpile canned goods, 11% were preparing to buy generators and woodstoves, and 13% were going to purchase "alarm systems, fencing, and firearms."[5] Another article in the *Wired* special issue said: "If a Y2K crisis occurs...citizen participation would be crucial, because government agencies will be spread too thin." The article went on to quote Steve Davis, a Montgomery County, Maryland, budget manager who has focused on Y2K issues since 1996, who said, "We've determined that in any of the worst-case scenarios, we can't shelter and feed the masses if there are power outages or food shortages. People are going to need to take care of themselves."[6]

Although community preparedness initiatives are reported to be well advanced in some parts of the US, the rest of the world is said to be lagging behind. An article in the *Guardian Online* of May 27, 1999 featured Angela Henderson, a Y2K Community Action Network member, who said: "The model we'd like to see adopted here is that groups set themselves up, using existing structures like our neighbourhood watch for example, to identify local people who would be vulnerable if there were power cuts...if the worst case scenario

unfolds, in the middle of winter, then people can help each other."[7]

References

1. When complex systems fail - Margaret Wheatley, January 1999
    http://www.berkana.org/articles/complexsystems.html
2. System error - *GQ*, February 1999
3. Life in the dark - *Wired*, April 1999
4. The suburban survivalists - Sunday *Times*, January 3, 1999
5. 31.12.99: the Y2K nightmare - *Vanity Fair*, January 1999
6. Powerless - *Wired*, April 1999
7. Digging in for the digital doomsday - *Guardian Online*, May 27, 1999

'Awareness' is followed in the full report by 'Preparations', 'Problems & Solutions', and 'Effects'.

Please contact: sales@trendmonitor.com

Jan Wyllie
Trend Monitor "The Information Refinery"
3 Tower Street
Portsmouth, Hampshire
PO1 2JR, UK
Tel: +44 (0)1363 881017 or +44 (0)1705 864714
Email: jan@trendmonitor.com
Web: http://www.trendmonitor.com/

"only what you need to know"