NATO OTAN

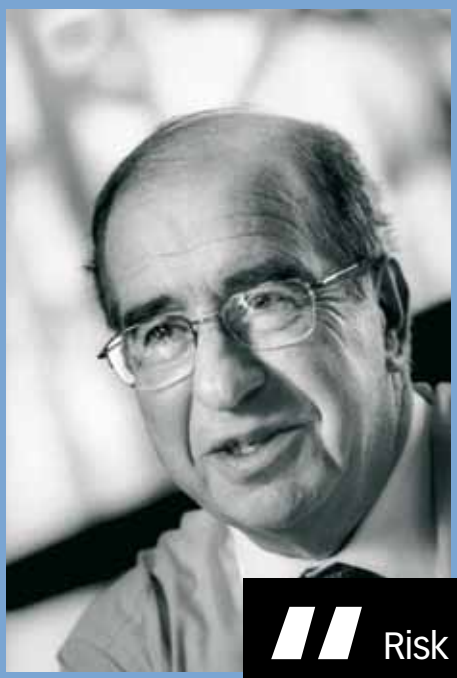
LLOYD'S

LLOYD'S 360° RISK INSIGHT

MANAGING RISK IN THE 21ST CENTURY

The risk environment is changing faster then ever before. Global insurance market Lloyd's and NATO have collaborated to examine how business leaders and governments can tackle future emerging risks.

These articles do not necessarily represent the opinion of the Financial Times, but the opinions of Lloyd's and the contributing authors.



VIEWPOINT

Lord Levene, Lloyd's Chairman

Lloyd's recently asked business leaders which risk keeps them up at night. The answer was overwhelming: "the economic climate". Given the global economic recession this is not surprising, but this publication – based on a 360 Risk Insight seminar jointly hosted by Lloyd's and NATO should remind the business community that the other big issues; climate security, cyber crime and piracy haven't gone away. If a lasting feature of this economic crisis will be to improve risk management, my advice to industry is to ensure that these issues are on your boardroom agenda. In all three, we are seeing a series of incremental but insidious changes that have the potential to disrupt the way we do business.

> "Risk Management needs to move from the backroom to the boardroom."

The overriding impression I took from the seminar is that we are looking at a pretty scary future of floods, droughts, kidnaps and ransoms, identity fraud and computer scams. Faced with such a prospect, people and businesses are divided into two camps; those who think that there is nothing they can do, that they are too small or insignificant to solve these problems and, on the other hand, those who will adapt themselves to change and influence the future.

Our seminar gathered people from very different fields. A polar explorer, a security expert from BT, the Estonian Defence Minister and a Lloyd's piracy underwriter all shared a stage. The variety was deliberate, because even a cursory glance at some of these problems reveals a complex cast of characters. We could have found the event was a Tower of Babel, with us all speaking different – and untranslatable - languages, but that wasn't the case. People listened hard, rolled up their sleeves and looked for solutions. Some important trends emerged:

- We need greater investment in research and development, particularly on climate change and digital threats.
- Risk management needs to move from the backroom to the boardroom. We have acres of data at our disposal, but too few decisions.
- We need pragmatic policies that reflect reality. Climate change is irreversible. Cyber space is here to stay. Failing states will breed more pirates. Action is necessary.

Lloyd's teamed up with NATO in part because when things go wrong in a very big way, NATO and Lloyd's are on speed dial. But the partnership reveals more than a common interest in risk management. Business and governments need each other to manage each of these risks. Take piracy – without the insurance provided by Lloyd's or the security of NATO's patrol vessels, shipping could seize up in the Gulf of Aden.

Globalisation has re-distributed power. This doesn't mean that governments are less important, but it does mean they will need to bring business to the table to work out how to manage complex risks. This publication sets out why business needs to accept the invitation.

IMPACTS OF CLIMATE CHANGE ON BUSINESS AND SECURITY

In just a few weeks, at the UN Climate Change Conference in Copenhagen, world leaders will pose for the customary "family photograph". Will this be one that we want to keep in the albums of history, or will it endure as a reminder of the day when the world failed to tackle global warming?

Our 360 Risk Insight panel of Pen Hadow, David Smith and Nick Mabey examines whether the road to Copenhagen is paved with more than good intentions, and why business and security communities must prepare themselves, regardless of the success or failure of the summit, for massive changes ahead.

The world is changing

Presentations at Lloyd's rarely begin with a video clip of "me at work". But then most people's average day doesn't involve a swim in the Arctic Ocean. Explorer Pen Hadow has just returned from the Arctic and wants to share his experiences and observations from the Catlin Arctic Survey. The video deftly sums up his main point: the ice at certain times of year is thin enough and sparse enough to swim through. The ice cap is shrinking, and more quickly than we first thought. Hadow explains that we have already lost 40% of summer ice cover, an area the size of the United States, and what is left is thinner.

Hadow, who will present his findings in Copenhagen, wants to drive home to the business and security communities that the loss of ice will affect far more than the Arctic region. "As the Arctic opens up, and it is going to open up, I think there is going to be a mass-scale change of vision in how we regard our planet. It is not going to be seen as this irrelevant, inaccessible, dead-end place".

NATO Secretary General Anders Fogh Rasmussen agrees, setting out how the opening up of shipping channels in the Arctic and potential resource exploration will, very directly, change the relationship between human beings and the Arctic.

Both men understand that this is not just about the ice caps, or as Hadow calls them "the white bits on a children's globe". There is a connection between the white bits and the Equator, which in turn drives our weather systems. The melting ice will lead to more extreme weather events closer to home: storms and flooding, droughts and water shortages. But how will this impact on business and security?

Arctic opportunities

In September, two commercial ships used the Arctic to transport goods from South Korea to the Netherlands. This journey feels significant, the beginning of a new era, or a symbol that something we had taken for granted, that the ice caps were fixed, monumental and permanent, has changed. Many of us dimly recall learning at school about the search for the Northwest Passage linking Asia and Europe – tales of maritime daring and disaster as, for centuries, ship after ship failed to make it through the ice.

Of course, the Arctic remains a hostile, high risk and difficult environment, for shipping and for energy exploration, but it is becoming accessible.

The opening of something that has been locked tight to every previous generation requires sensitive and careful handling by the businesses that want to operate in the region and by the Arctic states, which are busy staking claims to the newly accessible seabed and the precious resources that lie beneath it.

> "The secret to survival as the fittest, is to get ahead of the climate curve and exploit the opportunities before your competitor does."

The de-industrial revolution?

Pen Hadow calls the Arctic the "visual manifestation" of global warning, but stresses that change will happen everywhere. David Smith, Chief Executive of Global Futures and Foresight, argues that "we are at a point of discontinuity", in other words that climate change has led us to a tipping point where nothing will ever be the same again. Strong words, and Smith takes a Darwinian position, whereby companies that recognise change is inevitable will outclass competition that is slower to grasp the point.

The secret to survival as the fittest is to get ahead of the climate curve and exploit the opportunities before your competitor does. Significantly, panelists predict enormous

investment in non-polluting infrastructure and a growth in green consumer spending. According to Smith, ethical spending has held up well during this recession.
Nick Mabey, of the think-tank E3G, estimates that "the transition to a low-carbon economy will require investments worth $1.3 trillion up to 2030". Smith assumes that a massive change in public thinking will drive businesses to ensure that their brand is greener than their competitors'. A race to the top will ensue, with

> "Climate change is not going away, so we need to focus on adapting our businesses and homes to reduce our vulnerability."

companies devising tighter, cleaner supply chains. Additional climate change wins, argues Smith, will include the ability to recruit the best talent, to keep on the right side of regulators and even to secure investment.

Is Smith right to predict such a profound shift in public expectations? Mabey thinks so, he senses activism in the air and predicts, in the weeks leading up to Copenhagen, that "a tsunami of public opinion is about to land on politicians". He suspects that this is making some people nervous: "a lot of press releases are already being prepared to justify why Copenhagen can't work".

Climate change will act as a threat multiplier

Nick Mabey believes that one ray of light at Copenhagen will be unanimity on the global security implications of climate change. The premise is that scarce resources – not just oil and gas, but also water and basic food crops – will lead to instability between states and within individual countries. Mabey claims that security analysts are converging on a central scenario: the world will witness more instability, more internal conflict - more "Somalia-like" ungoverned places.

Given these trends, managing resources will require enormous amounts of preventive diplomacy. NATO Secretary General agrees that a discussion should begin on "how we – NATO as an organisation and individual Allies as well – can do better to address the security aspects of climate change".

Mabey is calling for sharper risk management of climate change, and urging all parties to consider the worst-case scenarios: a failure to agree low-carbon targets, or prevent deforestation or glide smoothly to a nuclear powered future.

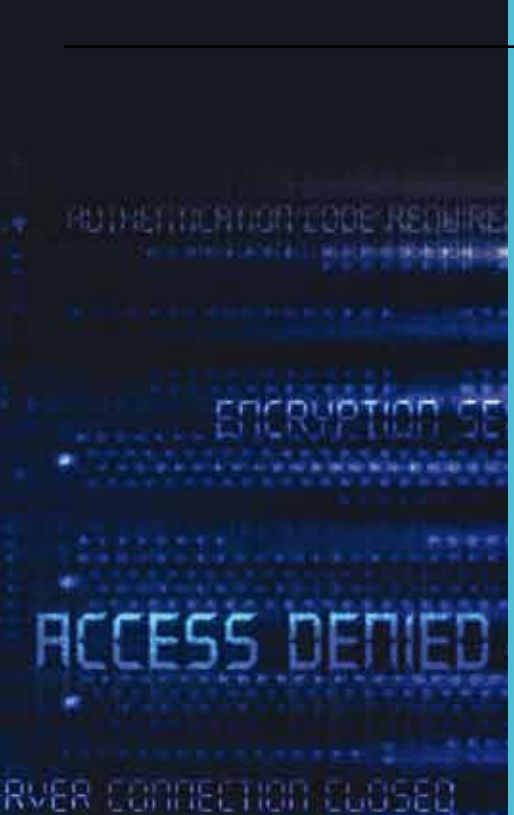
If the international community wants to avoid a breakdown in the security environment, Mabey is unequivocal that the world needs a zero-carbon energy system by 2050 with a carbon-free power system in developed countries by 2030. This calls for a quadrupling of governmental expenditure on research and development and a doubling of the rate at which advanced technology moves into the developing world.

Will this happen? Mabey and Smith fear a "greenwash", climate change speak for a fudge. Yet regardless of the hard outcomes in Copenhagen, the direction of travel is looking increasingly clear, with public debates springing up in such diverse places as China and Mexico. Mabey, however, wants to hear stronger voices from the security and business sectors in the lobbying ahead of Copenhagen, after all, he warns: "you are going to have to pick up the bill".

Whatever happens at Copenhagen, climate change will not stop

Our 360 Risk Insight panelists agree on the importance of decisive action at Copenhagen, but divide on the prospects of success. Perhaps the only person not tuning into what happens in the Danish capital this December is Mother Nature. Regardless of what is, or is not, decided, the ice will get thinner, crack and melt, and forests will fall prey to fierce fires. The overriding impression of this debate is the inevitability of a big shift in the way we live and the risks that we face. Lord Levene, Chairman of Lloyd's, argues for a "policy of pragmatism", accepting that climate change is not going to go away, and a focus on adapting our businesses and homes to reduce our vulnerability. Adaptation, claims Levene, ranges from "grand schemes" like the Thames flood barrier, to simple solutions, such as householders in flood zones "moving valuables upstairs".

Another conclusion from the debate is the urgent need for highly networked solutions, bringing in governments, security architecture, businesses and consumers. Pen Hadow ends his presentation by turning to the great and the good of the security and business worlds, arms stretched wide, saying "it is over to you now".



MANAGING CYBER RISK: FROM CYBER TERRORISM TO CYBER CRIME

In less than a generation, cyber space has gone from being a new frontier to an established city, where we shop, bank, trade and even govern. But for criminals, terrorists and hostile states, cyber space still bears the hallmarks of a frontier town, with inadequate policing, security or standards.

Our 360 Risk Insight panel of British Telecom's Ray Stanton and Estonian Minister of Defence Jaak Aaviksoo consider how businesses and governments can manage this growing threat.

An enemy within the PC

Cyber crime is not a niche business. It attracts a broad range of criminal activity from petty thieves and organised criminals to hostile states and terrorists. We all have information somewhere in our PCs or BlackBerrys that others would like to use for their own ends. The phishing attack at Yahoo, Hotmail and Google in early October, resulting in the loss of thousands of passwords, is the latest sign of the determination of organised cyber gangs to access our data. These groups are growing increasingly sophisticated. They will seize on times when our defences are at their lowest - during a flood or an earthquake - when IT departments are focused on restoring online services.

> "Without proper risk analysis, businesses are running a risk of their systems being compromised through the back door."

At another end of the crime spectrum, the 2007 cyber attack on Estonia showed similar trends of careful planning against clear targets. Government, industry and private internet sites were carefully identified to cause maximum disruption to the country. Many ordinary Estonians found themselves unable to go about their daily routines so, of course, they questioned the ability of their government to provide stability and security. Although the motivations of the commercial criminal and the hostile state are very different, our panelists identified some common defences against cyber attack.

Are you wearing a cyber safety belt?

Ray Stanton advises that "today, there are more compromised personal and business computers than two years ago" – a clear call for individuals and businesses to pay more attention to their cyber security.

Many of us underestimate the digital risks we run, or we think that there is nothing we can do to defend ourselves. This is actually not true. Basic security rules apply in cyber space just as they do when we drive a car. In a car we keep the brakes in good condition and ensure that the lights work. When operating a computer, we need to keep a constant eye on the virus guards and firewalls. A failure to do this can have disastrous results. For example Bank of America lost its ATM network due to a simple virus.

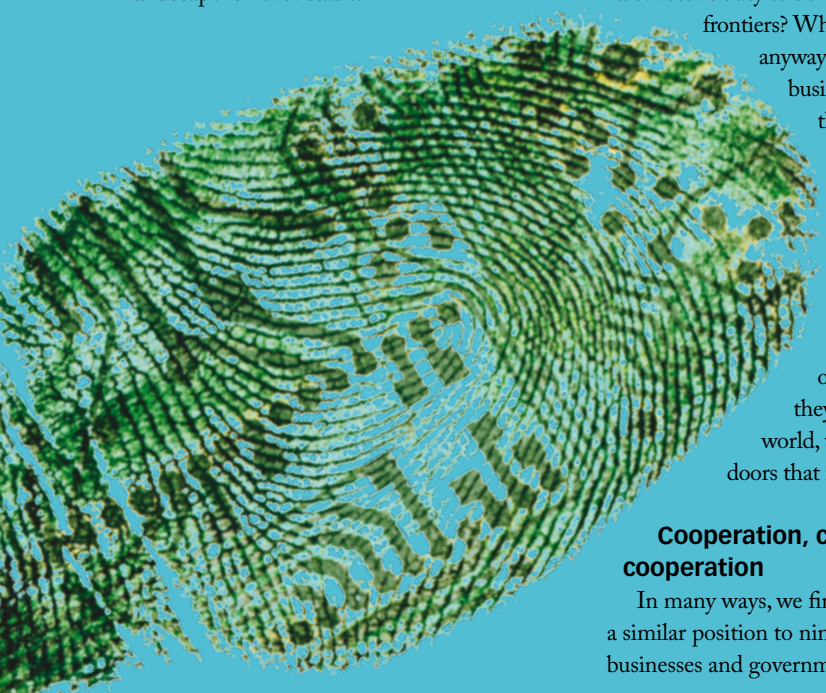
An important role for governments and businesses is to educate people about cyber risks and how to defend themselves from attack.

But we should guard against a belief that producing a leaflet or a training manual will solve all of our problems. Many people need to change their online behaviour and unlearn bad habits. Getting people to stop smoking or wear seatbelts were not easy tasks, but over the space of a generation, many people have ditched cigarettes and belted up, so it can be done.

Stanton predicts that individuals will increasingly buy their own end devices, BlackBerrys or PCs. Remote workers are already using machines which have not been bought or adapted by an IT department. Without proper risk analysis, businesses are running the risk of their systems being compromised through the back door.

Complex supply chains lead to what Stanton describes as 'deperimeterisation' – a long word meaning we do not know where our information boundaries lie. Can a modern company secure information all the way through its supply chain? Stanton believes that it can, but this requires highly focused risk management, concentrated on understanding what data is critical to a business.

A significant challenge is the sheer scale of people using digital technologies, or what Stanton calls the power of four: veterans, baby-boomers, generation X, and the Y-generation. They all have different educational needs. In addition, the Y-generation of people in their teens and twenties demand more online services which creates the commercial imperative for constant digital innovation. So the risk landscape is never static.



Balancing security and innovation

It is impossible to stop, or even slow down the speed of innovation. Businesses that try to do this may find themselves at a disadvantage – everyone in the workplace knows how frustrating it is to be denied the latest technology or access to certain sites and services. However, businesses need to keep a close eye on security.

At the international level, the Council of Europe Convention on cyber crime aims to stimulate countries to monitor, patrol and regulate their cyber space, and to cooperate with one another. Jaak Aaviksoo believes cyber space must continue to be "a free domain, where civil rights and liberties remain protected".

> "Digital threats need a focused, long term risk management strategy, with a heavy emphasis on business continuity."

But the international dimension remains a thorny one, even in the case of a hostile attack from another state, leaving NATO's legal team with a series of difficult issues. Can a computer be considered a weapon? Is a cyber attack an armed attack? Do NATO allies have a collective duty to defend each others cyber frontiers? Where are these borders anyway? Individuals and businesses may well have the easier task. They can make real strides, simply through surveying their digital space in the same way as their physical space. No one would leave the door to their house or business open when they go out, and in cyber world, there are usually several doors that need to be locked.

Cooperation, cooperation, cooperation

In many ways, we find ourselves in a similar position to nineteenth-century businesses and governments during the pioneering stages of the industrial revolution. An overwhelming amount of invention in a short period of time led to an initial phase of barely regulated, highly localised innovation. Railways ran on different gauges and there was a general lack of standardisation. Of course, the situation settled in the end and common practices, not least safety standards, were established. Essentially, the pace of change slowed so that the predecessors of today's risk managers could catch up. But it took an enormous burst of energy and a conscious attempt at better coordination. Now we need to do the same.

For Jaak Aaviksoo, the most important factor in Estonia's stand against the 2007 attack was not its formal defence hierarchy, but the informal cooperation between experts in government, banking and telecommunications companies. The actual attack has sharpened minds. Aaviksoo believes "different states and non-state organisations have decided to grab the ball and run with it". But he sounds a warning bell that often there is "little coordination, with civilian and military structures working in parallel, with limited communication".

Prepare for the improbable

Jaak Aaviksoo, who has experienced the front line of a cyber war, sums up his approach: "It is the impact of highly improbable events which will change our lives, sometimes dramatically." Good risk management does not only cover what is likely, but looks at the big bang events that change everything. Digital systems, which interconnect a myriad of systems, processes and people could make a very big bang indeed, so we need to be bold in thinking the unthinkable. We can draw a number of conclusions. Digital threats need a focused, long-term risk management strategy, with a heavy emphasis on business continuity. Failure to plan for the worse can have serious effects - disruption to IT systems caused by a subsea earthquake left traders in financial institutions unable to work for hours. Boards need to get involved, not least because, in the UK at least, data protection laws could leave them responsible and accountable for a loss of data. Proper risk management could quite literally, save you from jail.

Lloyd's new report, Digital Risks, can be found at www.lloyds.com/emergingrisks

TACKLING PIRACY: TRENDS, ISSUES AND SOLUTIONS

Lloyd's has dealt with the age-old problem of piracy for centuries, but the daring of new-age pirates with their speedboats and machine guns has captured the headlines and sent fear rippling through the marine community. With hundreds of ships held hostage every year, pirates have once again stepped out of the pages of children's fiction and into a brutal new reality.

Efthimios Mitropoulos, Secretary General of the International Maritime Organization (IMO), and Rupert Atkin, Chief Executive of the underwriting firm, Talbot, consider the impact of modern day piracy on business.

Pirates of the Gulf of Aden

No one would expect a city CEO to be worrying about pirates, but Rupert Atkin has watched piracy grow and become increasingly sophisticated over recent years. Have we responded accordingly? Merchant seamen, understandably, do not want to carry arms. So they have used a variety of tactics from fixing barbed wire to their ships to using fire hoses and loud horns. Not hugely different from sailors in the last Elizabethan era, who greased the decks and sprinkled them with dried peas and broken glass. The message is clear: once a pirate has boarded, the remedies look pretty desperate. So the challenge is to stop them getting on deck in the first place.

Efthimios Mitropoulos provides a quick geography lesson. Global piracy hotspots have switched from the Straits of Malacca, Singapore and the South China Sea to the coast of Somalia and the Gulf of Aden, and now into the Horn of Africa and the wider expanses of the Western Indian Ocean.

Modern day pirates are not just extending their geographical reach. Mitropoulos points out that they have become bolder, better armed and that attacks have grown dramatically in both number and ferocity. The Somali pirates are a long way from the treasure-seeking buccaneers of Hollywood films. Their methods, as they take on multi-nationals, are brutal and direct – hijacking ships and holding their crews against huge ransom demands. "The average ransom last year was between one and two million dollars, and this has gone up to between two and three million" explains Atkin.

To date, this has resulted in the injection of some $90 million into the Somali economy. For the struggling communities in this part of the world, which a bitter civil war has left with no effective form of government or justice, it is easy to turn a blind eye to the pirates' activities.

> "Pirates have become bolder, better armed and equipped and attacks have grown dramatically in both number and ferocity."

Atkin describes how, when early Somali pirates returned home, their families were missing, having been kidnapped while they were holding up a ship. The pirates have got round this problem by making deals with local communities to protect their families whilst they are at sea. This has resulted in pirates funding not just the growth of 4x4 vehicles in the Somali wilderness, but also basic services such as clean water. The more reliant that Somalia becomes on this money, the less likely a permanent solution looks.

Cost of piracy

Ask the crew of the kidnapped vessels what the human cost of piracy is, after they have been held hostage for weeks on meagre rations. Consider the impact on consumers across the world. Shipping is about taking products from A to B, and if that journey is prolonged, or a cargo is lost through a hijack, then costs inevitably rise. The average cost of a hijack is $1,000,000 per ship. These expenses are currently being born by the shipping and energy sectors, but if the problem persists, Atkin advises that "ship-owners will eventually pass on these costs".

> "Until the international community finds the tools to address failing states, we can only treat, not cure, this modern day outbreak of piracy."

The astonishing growth of attacks by Somali pirates has not gone unnoticed in neighbouring countries. Yemen, which has Al-Qaeda and secessionist issues itself, is potentially the next source of problems. Looking at worst-case scenarios, Atkin asks how a shipping boycott of the Gulf of Aden, and hence the Suez Canal, would affect Egypt's economy and its fight against extremism.

Seen in this way, piracy quickly becomes a universal concern, with severe impacts on global trade and regional stability.

Short-term military solutions

The International Maritime Organization (IMO) has been working to find a solution to piracy since the 1980s, in conjunction with the United Nations, national governments and other political and defence organisations, such as the European Union and NATO.

Efthimios Mitropoulos believes that this grand alliance is making headway. "The response to piracy has been one of the great examples of international cooperation in the modern era," he says, with a degree of pride, noting that national Navies from every point of the compass are working together.

The IMO is working with the military to protect shipping routes and educate them on preventive, evasive and defensive measures. Mitropoulos advises ships sailing through the Gulf of Aden to contact coordination focal points, to use the transit corridor and to travel in groups. The Secretary General and Rupert Atkin agree on the need for punitive measures against the pirates. "Because legal prosecution is expensive and nobody really wants the pirates either in their jails or seeking asylum in the event that the legal process fails, they are often just simply disarmed and handed back" explains Atkin.

The IMO has created the Djibouti Code of Conduct, which aims at cooperation between signatory states on the arrest and prosecution of pirates, as well as rescue work. Unsurprisingly, with so many different states and international actors, finding the right legal framework to close up the loopholes that allow pirates to return, time after time, to their ships, is a major challenge.

Long-term solutions

Protecting merchant vessels through the Gulf of Aden, and ensuring that more pirates face justice are short-term goals. The long term solutions lie inland, in the struggling state of Somalia. Everyone agrees that once onshore, the pirates face a bleak and insecure future in a country with no functioning courts, frequent fighting between rival warlords and little opportunity for regular work. Until the international community finds the tools to address failing states, we can only treat, not cure, this modern-day outbreak of piracy.

Email 360@lloyds.com to register for information from Lloyd's 360 Risk Insight, including regular newsletters, events and reports on emerging risks.