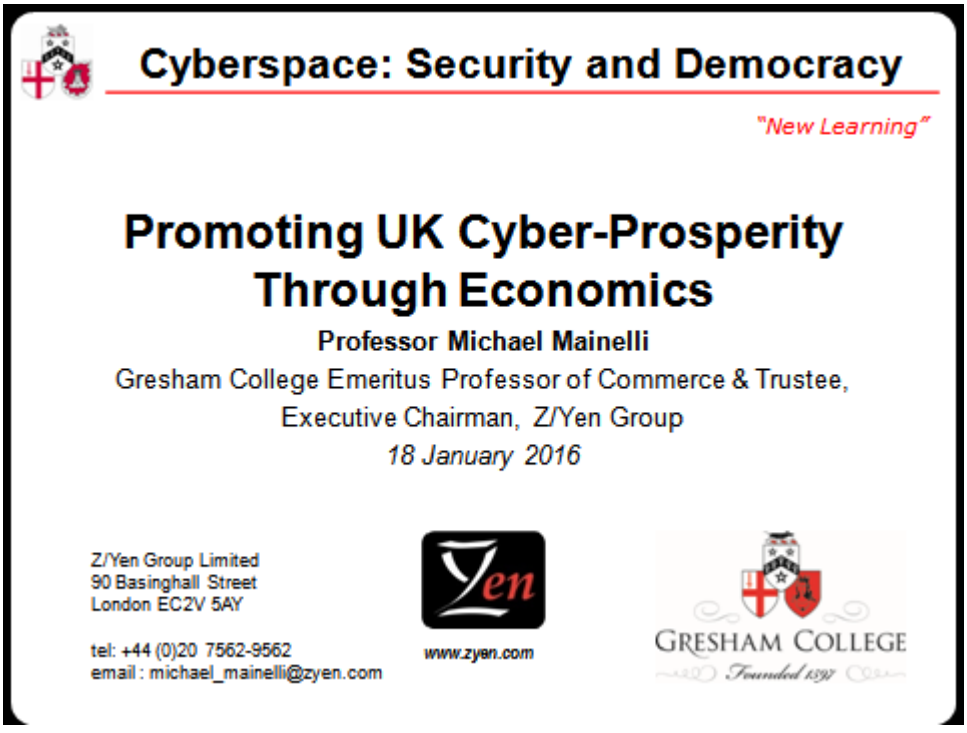
"Promoting UK Cyber-Prosperity Through Economics"

Professor Michael Mainelli
Gresham College Emeritus Professor of Commerce & Trustee,
Executive Chairman, Z/Yen Group
Monday, 18 January 2016
Barnard's Inn Hall, London EC1N 2HH

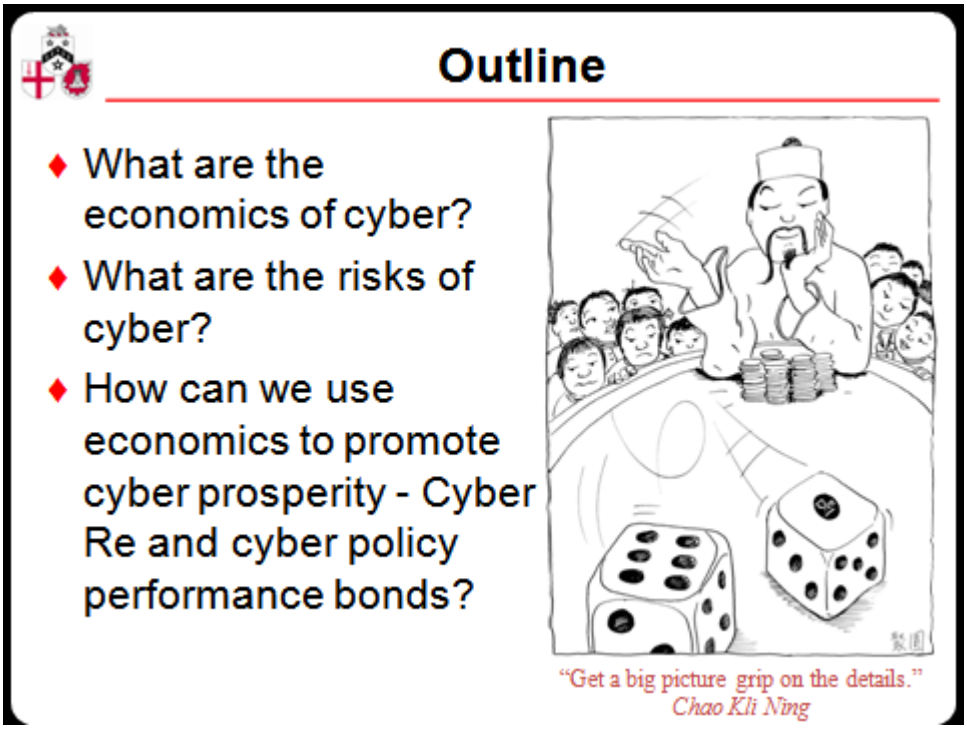
recording available at
http://www.gresham.ac.uk/lectures-and-events/cyberspace-security-and-democracy

Overview

In the face of rapidly growing cyber-risk, the tools of public and private economics can play a major role. Two such tools deserve greater attention, insurance and policy performance bonds. Making 'cyber' a 'normal' insurable risk by helping insurers insure themselves to insure others should aid UK cyber-prosperity. This lecture explores cyber insurance and the possible role of a government sponsored (though not government underwritten) Cyber Re. Cyber policy performance guarantees might also have a role to play in assuring business of government commitment, as well as helping to underpin cyber insurance. Both ideas might help democracies handle the security risks of cyberspace.



Good afternoon Ladies and Gentlemen. There are many perspectives on cyberspace from technical to social to security to democracy. This afternoon I would like to explore the economics. I intend to emphasise the way in which economics might be deployed to help free market economies towards cyber prosperity.



Much of this talk melds two pieces of work. The first piece of work was a report published last year, "Promoting UK Cyber Prosperity: Public Private Cyber Catastrophe Reinsurance". The second piece of work is our ongoing examination of money and government finance within Long Finance. Long Finance is a Gresham College, City of London Corporation, and Z/Yen initiative to address the question, "When would we know our financial system is working?"

I'll attempt to explore three questions in my thirty minutes:

- What are the economics of cyber?
- What are the risks of cyber?
- How can we use economics to promote cyber prosperity?

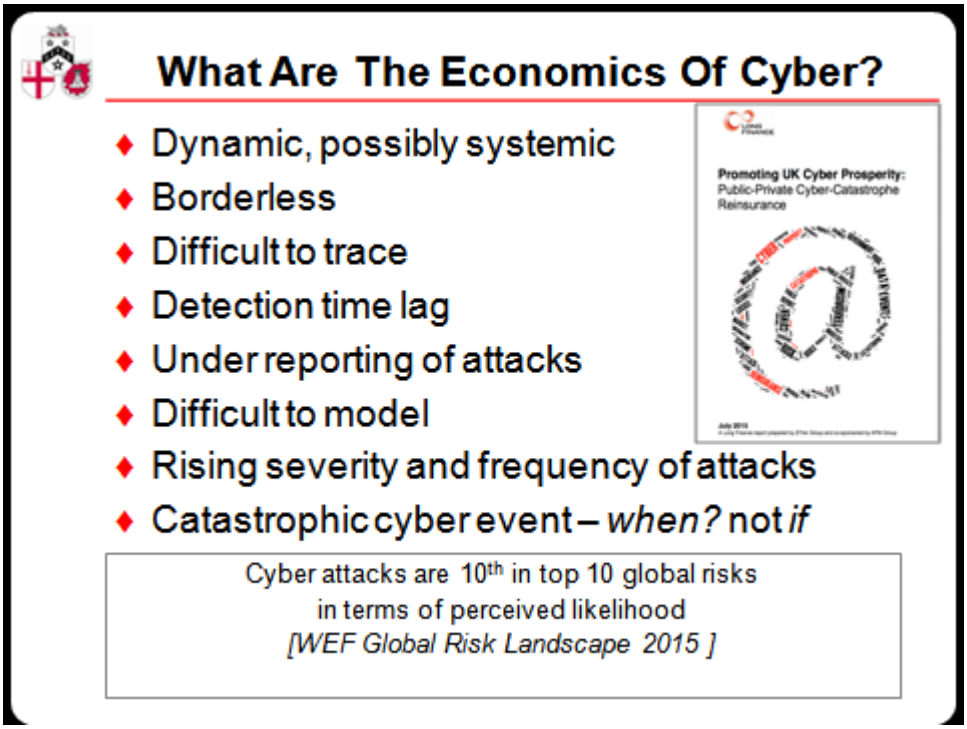
Before tackling the questions, I thought I might just touch on my background. 'Cyber' has become shorthand for the combination of computers and networks that increasingly touch every aspect of our lives. I was lucky enough to have the opportunity to learn programming in the early 1970s. I was even luckier to get on the internet in 1976. I've seen four decades of change in the combination of computers and networks. It started with wonder. The basic engineering pleasure of successfully connecting and transmitting filled us with glee.

The information and communications revolutions are still awe-inspiring, but now tinged with many fears from poor security to police state surveillance, from over-commercialisation to the destruction of long-established industries, from idiocracy to rule of the masses, and from servitude to slavery by artificial intelligences. This short talk will examine two economic approaches that might help improve our security.

What Are The Economics Of Cyber?

90 Basinghall Street
London EC2V 5AY
United Kingdom

Risk/Reward Managers
tel: +44 (020) 7562-9562
fax: +44 (020) 7628-5751
www.zyen.com

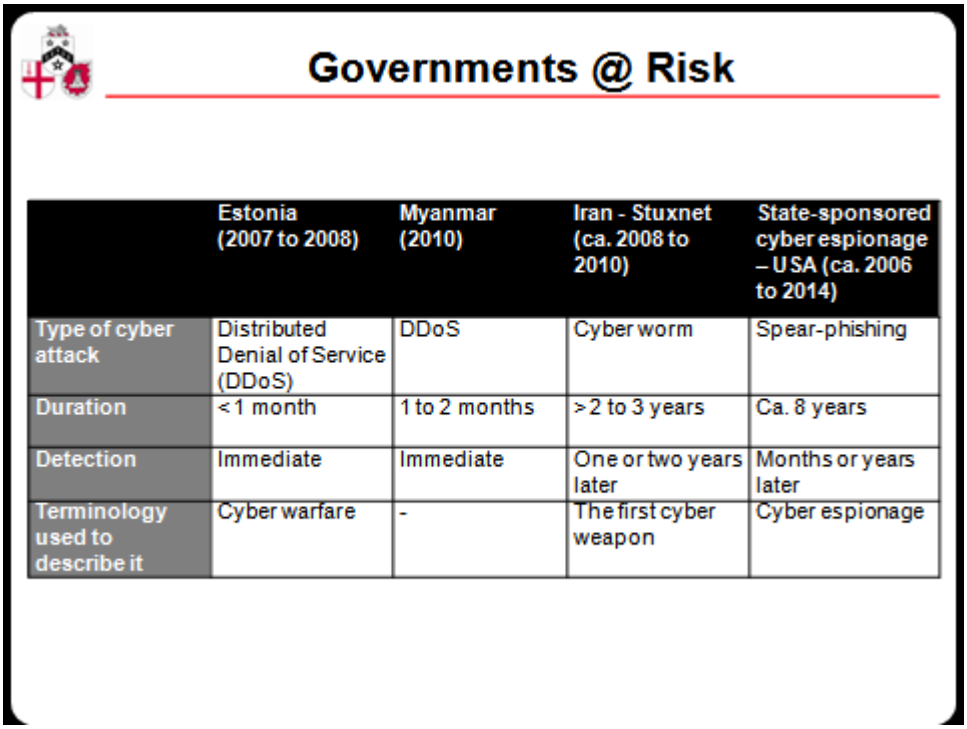


The direct internet economy in the UK is estimated at approximately 8%. Our dependence on this sector is enormous. Last year, the then UK Business Secretary Vince Cable said "The UK has a world-leading digital economy, growing three times as fast as our overall economy and employing over a million people. Our businesses earn £1 in every £5 from the internet, so it's vital that we work with them to combat online crime, and make sure large and small firms alike are protected."

I will skip the obvious swiftly - ***modern society cannot function economically without computer networks***. Looking to the future, the EU points out that business clearly sees information and communications technology as crucial, representing 17% of total European business R&D.

90 Basinghall Street
London EC2V 5AY
United Kingdom

Risk/Reward Managers
tel: +44 (020) 7562-9562
fax: +44 (020) 7628-5751
www.zyen.com



Governments @ Risk

	Estonia (2007 to 2008)	Myanmar (2010)	Iran - Stuxnet (ca. 2008 to 2010)	State-sponsored cyber espionage – USA (ca. 2006 to 2014)
Type of cyber attack	Distributed Denial of Service (DDoS)	DDoS	Cyber worm	Spear-phishing
Duration	< 1 month	1 to 2 months	> 2 to 3 years	Ca. 8 years
Detection	Immediate	Immediate	One or two years later	Months or years later
Terminology used to describe it	Cyber warfare	-	The first cyber weapon	Cyber espionage

Anyone using computers connected to networks is potentially exposed to cyber-risk, including governments as the slide indicates. In fact, the amounts already spent on defences for cyber-security already amount to some $75 billion in 2015, not counting the computational energy, people time, and other costs, such as storage and networking. But a case study of what the future holds, good and bad, is worth a small detour.

This past summer a North American energy insurer raised an interesting problem with us, particularly if you care about global warming. They were looking at insuring US energy companies about to offer reduced electricity rates to clients who allowed them to turn appliances on-and-off, for example a freezer. Now freezers in America can hold substantial and valuable quantities of foodstuffs, often several thousand dollars. Obviously, the insurer was worried about correctly pricing a policy for the electricity firm in case there was some enormous cyber-attack or network disturbance. The control systems are now as important as the power supply.

Take for example coming home to find your freezer off and several thousands of dollars worth of defrosted mush in your freezer. You ring your home & contents insurer who notes that you have one of those new-fangled electricity contracts. It was probably the electricity company. Go claim from them. You ring the electricity company. In a fit of customer service, they deny they had anything to do with turning off your machine, but, if anything, it was probably the freezer manufacturer who is at fault. The freezer manufacturer knows for a fact that there is nothing wrong except that you and the electricity company must have installed things improperly. Of course, you may not be all you seem to be. Perhaps you unplugged the freezer to vacuum your house and forgot to reconnect things. Or perhaps you were a bit tight on funds and thought you could turn mush into instant cash, or should I say frozen foods into liquid assets?

90 Basinghall Street
London EC2V 5AY
United Kingdom

Risk/Reward Managers
tel: +44 (020) 7562-9562
fax: +44 (020) 7628-5751
www.zyen.com

In future, machines will make decisions and send buy-and-sell signals to each other that have large financial consequences. We pointed out to our North American friends that they, the insurer, should perhaps tell the electricity company which freezers to shut off first, starting with the ones with the cheapest contents. With billions of people on the planet, we may need several tens of billions or even low trillions of ledgers recording all these transactions in case of dispute. My freezer-electricity-control-ledger, my entertainment system, home security system, heating-and-cooling systems, telephone, autonomous automobile, local area network, telephone recording, etc.

Perhaps the most significant announcement of 2015 was in January from IBM and Samsung. They announced their intention to work together on mutual distributed ledgers (aka blockchain technology) for the Internet-of-Things. ADEPT (Autonomous Decentralized Peer-to-Peer Telemetry) is a system jointly developed by IBM and Samsung for distributed networks of devices. They foresee a future of ten billion people with hundreds of networks, a trillion distributed ledgers.

So a first obvious interim conclusion, protecting ourselves from cyber disasters is crucial to our current and future economic success.

What Are The Risks Of Cyber?

Dirty Dozen Cyber Incidents 2015

Incident	Type	People Affected	Date
Anthem BCBS	Identity theft	80 million	January
Ashley Madison	Hacktivism	37 million	July
US Office of Personnel Management	Espionage	22 million	June
Experian & T-Mobile	Identity theft	15 million	October
LastPass	Fraud	7 million	June
UCLA Health	Identity theft	4.5 million	July
TalkTalk	Credit card fraud	4 million	October
Jeep	Mistake	1.4 million recalls	July
US Internal Revenue Service	Identity theft	>300,000	May
CVS Online Photo Centre	Credit card fraud	?	July
Kaspersky Labs	Espionage	?	June
US Central Command	Embarrassment	?	January

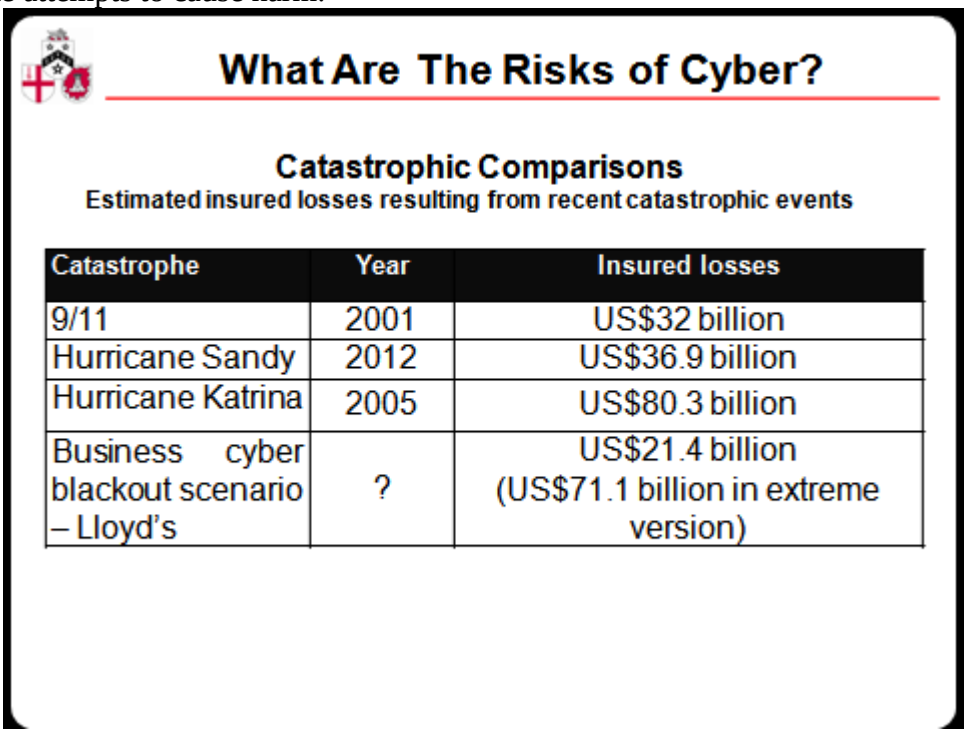
Cyber risk is increasingly perceived as a global risk to society and the economy. In the slide above three are espionage, four identity theft, and two credit card fraud. Let alone 'hacktivism'. 'Cyber attacks' rated 10th in the top 10 global risks in terms of likelihood and 'critical information infrastructure breakdown', and 7th in the top 10 global risks in terms of impact according to WEF's Global Risk Report 2015 (World Economic Forum, 2015). Insurance, banking and microfinance professionals across 50 countries rated cyber-risk as the fourth global risk in the latest edition of the bi-annual CSFI 'banana skins' survey

90 Basinghall Street
London EC2V 5AY
United Kingdom

Risk/Reward Managers
tel: +44 (020) 7562-9562
fax: +44 (020) 7628-5751
www.zyen.com

(CSFI, 2015). We have had a succession of corporate cyber debacles over the past year. Not least because the return on investment in cyber-crime is so good.

Cyber risk is a breach of "the confidentiality, integrity and accessibility of an entity's online or computer presence or networks and the information contained within" (Tendulkar, 2013). Associated risks and impacts can be due to human or system errors, natural disasters, and deliberate attempts to cause harm.



What Are The Risks of Cyber?

Catastrophic Comparisons

Estimated insured losses resulting from recent catastrophic events

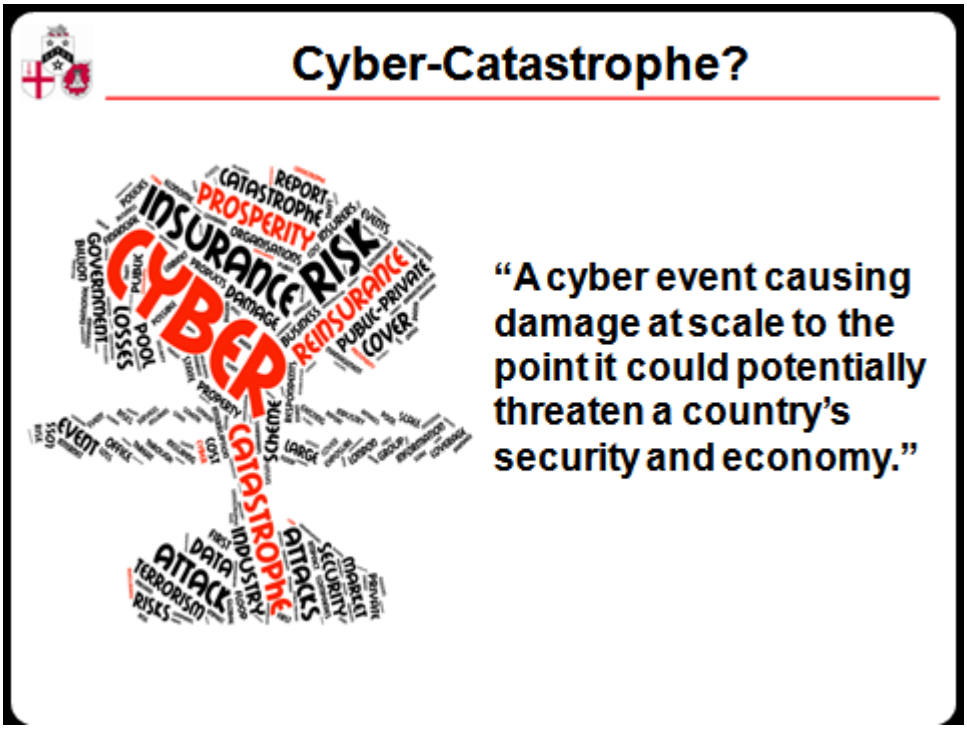
Catastrophe	Year	Insured losses
9/11	2001	US$32 billion
Hurricane Sandy	2012	US$36.9 billion
Hurricane Katrina	2005	US$80.3 billion
Business cyber blackout scenario – Lloyd's	?	US$21.4 billion (US$71.1 billion in extreme version)

Published jointly by Lloyd's and CCRS, a Business Blackout (2015) scenario explored the insurance implication of a major cyber attack, using the US power grid as an example. The report estimates the total impact to the US economy at US$243 billion, rising to more than US$1 trillion in the most extreme version of the scenario. The cyber attack scenario shows the broad range of claims (30 lines of business) that could be triggered by disruption to the US power grid, with the total amount of claims paid by the insurance industry estimated at US$21.4 billion, rising to US$71.1 billion in the most extreme version of the scenario (Lloyd's & CCRS, 2015).

A cyber catastrophe does not have to be the result of a malicious act. In September 1859, aurorae were seen around the world, northern lights as far south as the Caribbean and Senegal. People in the northeastern United States could read a newspaper by the aurora's light. Telegraph systems all over Europe and North America failed, in some cases giving telegraph operators electric shocks. Telegraph pylons threw sparks. Some telegraph operators could continue to send and receive messages despite having disconnected their power supplies.

90 Basinghall Street
London EC2V 5AY
United Kingdom

Risk/Reward Managers
tel: +44 (020) 7562-9562
fax: +44 (020) 7628-5751
www.zyen.com



With our tender nano-electronics, a geomagnetic storm of similar magnitude to the solar storm of 1859 (also known as the Carrington Event) could cause catastrophic damage to society – just consider all mobile phones being 'fried' at once. In 2008 the National Academy of Sciences estimated US social and economic costs in the range of US$1 trillion to US$2 trillion a year and suggesting that full recovery could take four to ten years.

So, a second obvious interim conclusion, cyber disasters could be economic catastrophes.

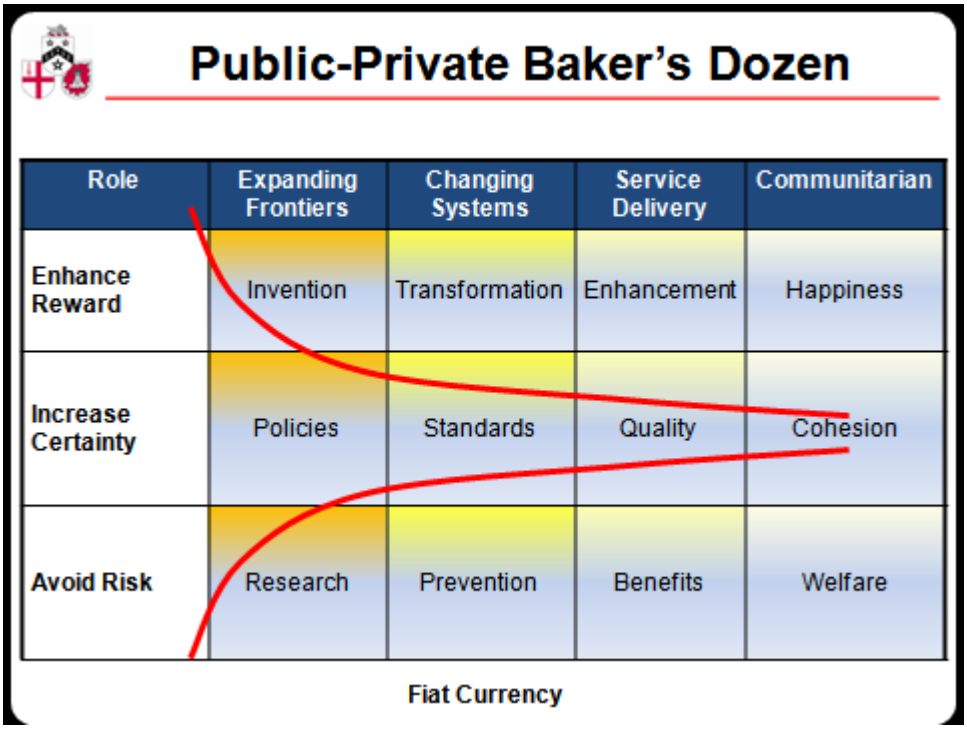
How Can We Use Economics To Promote Cyber Prosperity?

There are a number of interesting proposals and actions that have economic relevance. The government of Estonia has one of the finest national electronic identity schemes. To some degree the national distributed ledger and cryptography system is a reaction to the 2007 Russian attacks, but the Estonians turned risk into opportunity and now boast a highly efficient, digital nation based on letting citizens own their own data and providing them with the security and cryptography tools to manage their data and communicate with their government and each other. Another approach with economic motivation is the use of 'bounty hunters' for cyber weaknesses, or several proposals that email senders should pay, or risk non-delivery.

In 2012 I gave a lecture called "Risk, Equality and Opportunity: The Roles for Government Finance". The idea was to move from simple thoughts on tax and spend to exploring the rich variety of ways in which government finance interacts with markets. We ended on a framework of 13 areas of action for government economics. We also pointed out five roles for government action, as a benefactor, enterprise, guarantor, investor, or sorcerer's apprentice.

90 Basinghall Street
London EC2V 5AY
United Kingdom

Risk/Reward Managers
tel: +44 (020) 7562-9562
fax: +44 (020) 7628-5751
www.zyen.com



Our framework had a horizontal axis of four commonly sought outcomes in line with research into "Evidence of Worth". We postulated four generic outcomes.

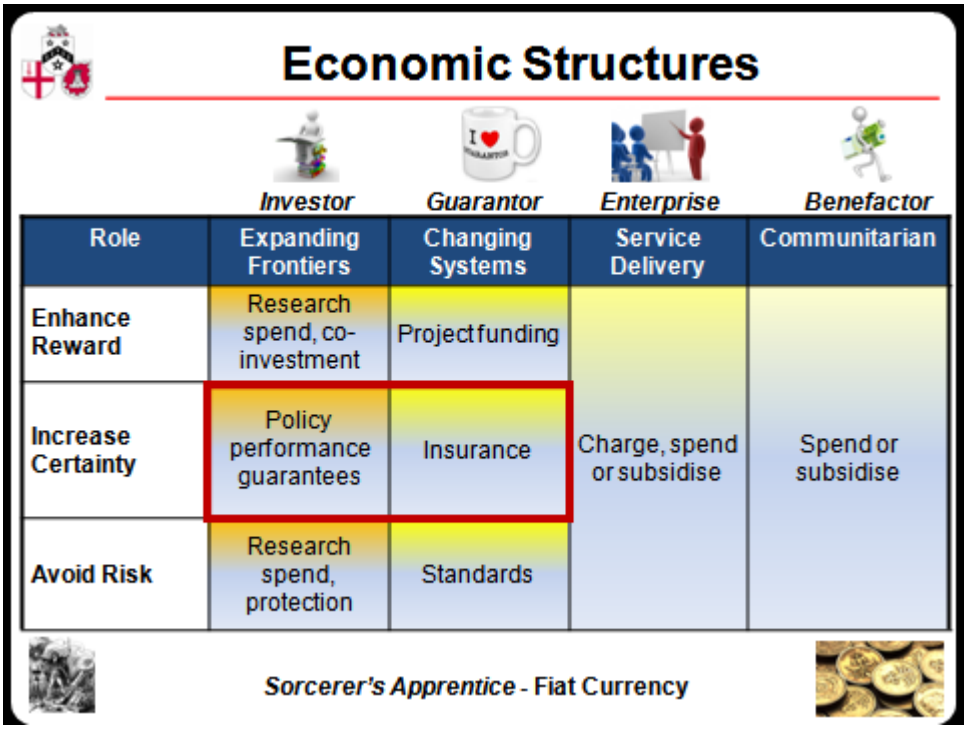
- expand frontiers to solve a problem - e.g. developing new drugs which might cure and/or prevent disease, or an anti-meteor protection system;
- change systems to develop markets or to release resources - e.g. the introduction of cap-and-trade carbon markets, or paperless government;
- deliver services to address the immediate need - e.g. delivering primary education or health;
- build community to help people deal with problems through communal activity – this may sound "Big Society" but has paid dividends in the past, e.g. vigilance against terrorism, tidy country campaigns, anti-drink driving and anti-smoking social influence messages.

The vertical axis distinguished three measures of success – enhance rewards, increase certainty, avoid risk. Combining the two axes creates this 12 part taxonomy of interventions. In each box we have a description of what government might do to influence the economy. In addition, the entire economic framework – in advanced nations at least – hinges on the role of government finance in managing the fiat currency, down here at the bottom of the slide. This gives us 13 generic actions, a baker's dozen of possible interventions.

In the diagram we move from high reward and high risk on the left, to low reward and low risk on the right. This slide emphasises one of the classic debates on the role of government – equality of opportunity versus equality of outcome. We might all agree to join forces to avert disaster by avoiding risk, but we are often divided politically on whether to enhance rewards or increase certainty.

90 Basinghall Street
London EC2V 5AY
United Kingdom

Risk/Reward Managers
tel: +44 (020) 7562-9562
fax: +44 (020) 7628-5751
www.zyen.com



The more alert among you may be getting a bit panicky about time, so I've simplified things a bit here. I might also point out that the UK government has already done a number of sensible things. Let's start on the far right and go left column-by-column:

- communitarian – actions include things like raising awareness, cyber vigilance, and helping to form associations and networks of academics or agencies, participating in international fora on cyber;
- service delivery – actions include things like training and courses on cyber, as well as public drills and national information centres;
- changing systems – quite a lot has been done on the top and bottom box, protection projects have been funded, and much work has been done on standards such as Cyber Essentials, ISO 27000, NIST, or CESG's 10 Steps;
- expanding frontiers – again, much research has been funded at the top to enhance rewards via developing a UK cyber market, and much research has been funded to avoid risk through cyber protection systems.

The government might argue they've done much. And I might agree, in 10 of the above 13 areas for action So, in the time available I'd like to explore two interesting areas where much more could be done, insurance and policy performance guarantees, and I'll leave a quick comment on fiat currency till last.

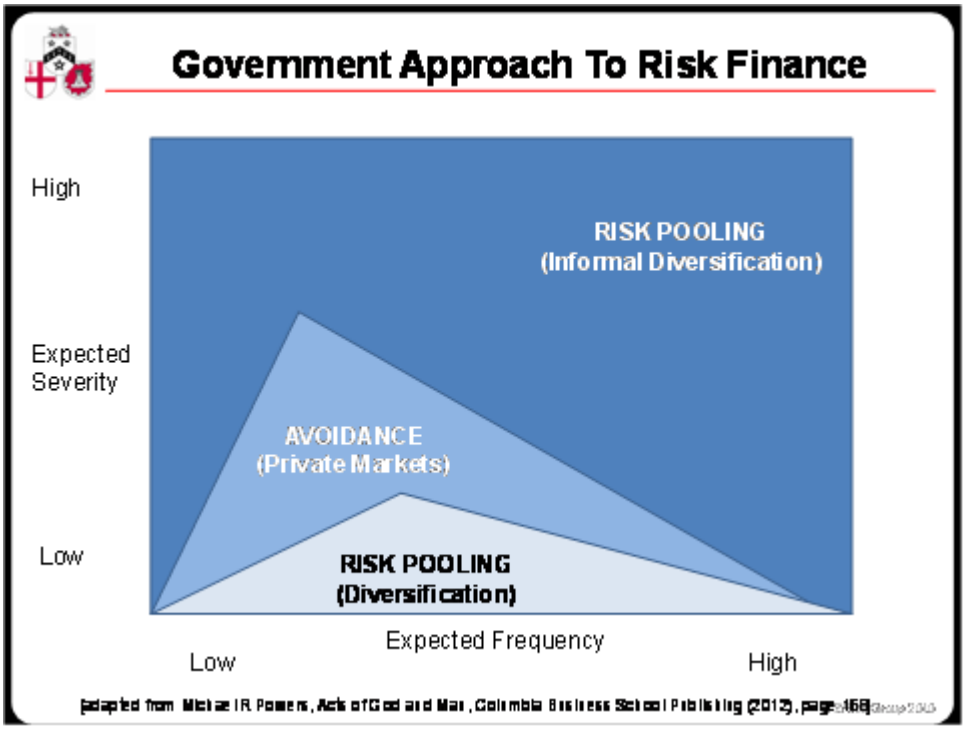
Insurance

In so many areas of risk, we know things are normal when we can insure against them. We face risks of fire, burglary, automotive damage, even life, but we seem to be able to structure managing these risks around insurance. Insurance is a mechanism that actually helps people learn about risk, and often why they report risk. Without insurance who would report burglaries in a high-crime/low-solved-crime area? Mary McAleese, the former

90 Basinghall Street
London EC2V 5AY
United Kingdom
Risk/Reward Managers
tel: +44 (020) 7562-9562
fax: +44 (020) 7628-5751
www.zyen.com

President of Ireland, made a wonderful speech on insurance that puts thousands of insurance marketing people to shame, saying:

"The certainty and confidence that insurance provision brings to all our daily lives, whether business or personal, enables us to breathe more easily, to find the confidence to let innovation flourish and to engage with the present and the future, chastened by the past but not allowing the fear of the possible to paralyse us in the present."
[speech to European Insurance Forum in Dublin, March 2010]



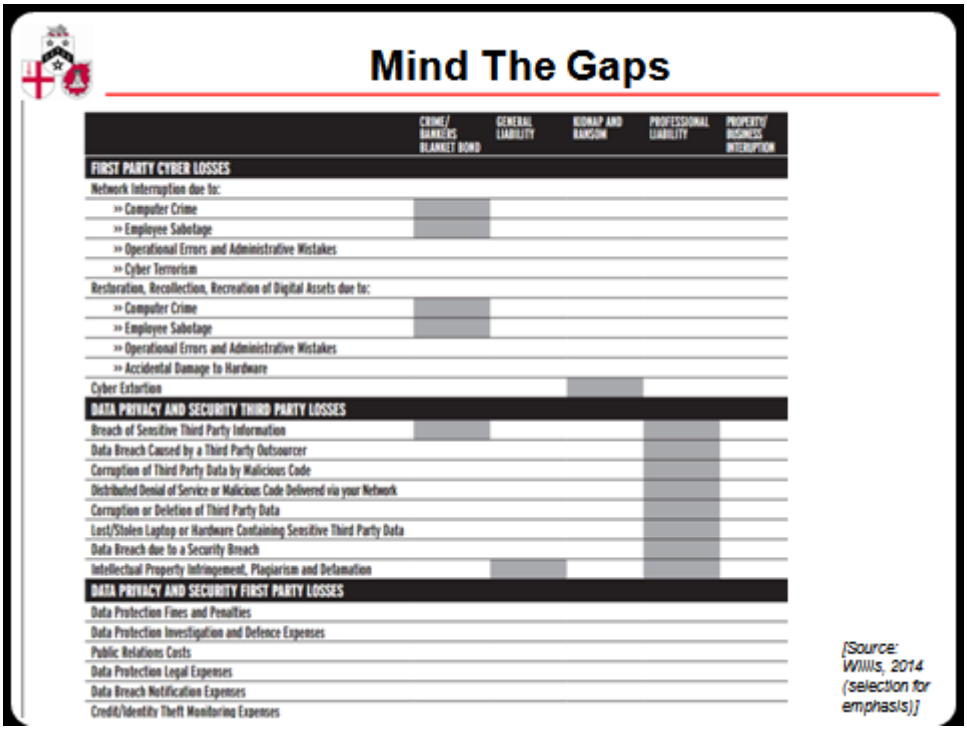
Government often acts as an insurer. John Locke was not as sunny as McAleese, writing, "Government has no other end but the preservation of Property." [John Locke (1632–1704), Second Treatise on Civil Government, Chapter 6 (written 1681, published 1690)] Pool Re provides a good example. Following the 10 April 1992 bombing which devastated the Baltic Exchange for shipping, insurers withdrew cover for acts of terrorism. In response, the UK government rapidly formed a new government reinsurer called Pool Re. Pool Re was emulated by the US after 9/11. Pool Re has been particularly well run over twenty years, remaining in significant surplus and supporting a broad property market. Further, it was set up with the aim of attracting other reinsurers into the market, at which it has also been successful. Pool Re is an example of the government spending virtually nothing but achieving a lot through finance.

Some folks counter that extreme event insurances raise contingent liabilities on the government's balance sheet. A contrary response is that many of these outcomes, cyber catastrophe or defunct pensions for example, will wind up on the government balance sheet if they occur, so insurance suggestions are good ways of using finance to make markets move outcomes in the right direction.

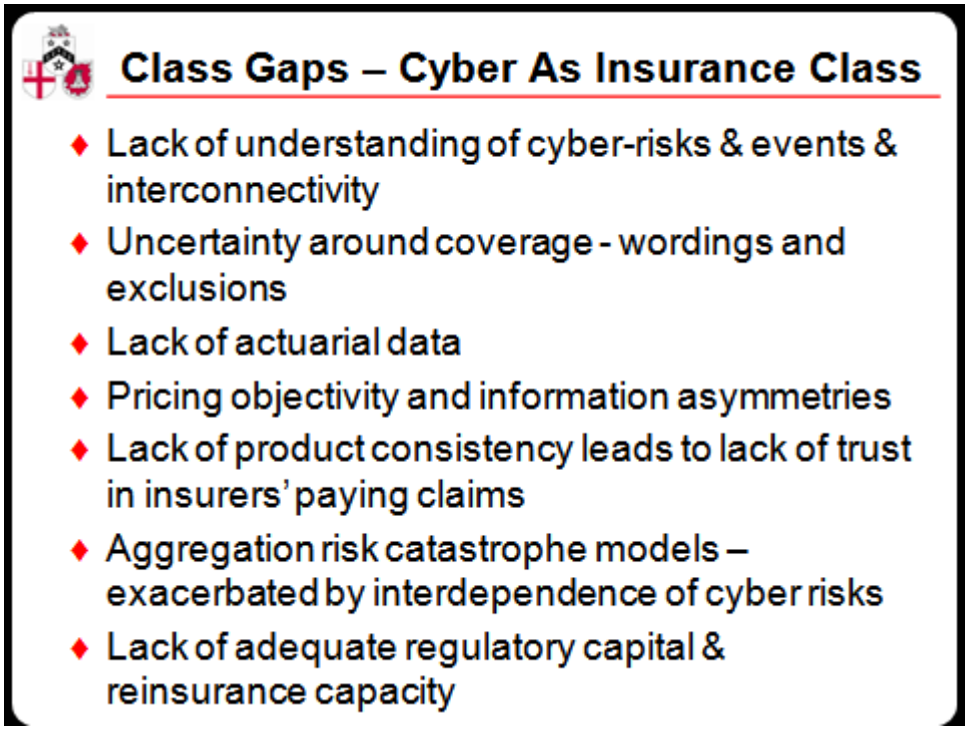
90 Basinghall Street
London EC2V 5AY
United Kingdom
Risk/Reward Managers
tel: +44 (020) 7562-9562
fax: +44 (020) 7628-5751
www.zyen.com

An interesting point arises when contrasting commercial and government approaches to insurance. A commercial approach by insurers works on risk selection. Many risks can't be insured or insured for reasonable cost, so risk control is the dominant approach. Once risk can be transferred, people hedge, typically via derivatives. If the risk can be pooled, then people use insurance.

"Unlike an insurance company, a national government cannot actually avoid any particular category of risk. Therefore, all exposures in the top-most region (with high expected severities, whether associated with low or high expected frequencies) must be accepted, albeit reluctantly by the government. However, because of the political difficulty associated with setting aside sufficient financial reserves for these costliest of exposures, the government will tend to address them only as they occur, on a pay-as-you-go basis. In the bottommost region, the government can take advantage of the likely presence of many similar and uncorrelated claims with low expected severities, so this region is much like the corresponding region for insurance companies. Here, the government sets aside formal reserves for various social insurance programs (e.g., pensions, health insurance and unemployment/disability benefits). Finally, in the middle region, the government typically tries its best to avoid these risks by encouraging firms and individuals to rely on their own private insurance products (but naturally, does not always succeed)."
[Michael R Powers, ***Acts of God and Man***, Columbia Business School Publishing (2012), pages 168-169]



So what is the current state of cyber insurance? Spotty. Still in its infancy. In March 2015, Marsh and HM Government published a report exploring how the insurance industry might help make UK companies more resilient to cyber threat. Recognising the potential for cyber attacks to cause costly and public disruption, the report noted the lack of awareness on cyber insurance products and the low level of cyber insurance cover (Marsh & Cabinet Office, 2015). Willis produced a note showing the enormous gaps above.



Circa 30% of major companies in the USA have cover versus 5% in Europe; in the UK it's around 2% for large organisations, close to 0% for SMEs. The US market is perhaps US$2.5 billion of gross premium, while the European market is about a tenth the size, US$150 million to US$200 million gross premium. Quite a bit of international confusion results from much of the US cyber insurance really being insurance for the administrative costs of following US data breach legislation, which requires an often ineffectual postal notification of the occurrence of the breach. When this type of local market insurance is removed, the US market resembles Europe, with great difficulty obtaining business interruption and third party liability. Quite rightly, insurers are taking a cautious underwriting approach with relatively high deductibles, low limits, and high comparative premiums.

90 Basinghall Street
London EC2V 5AY
United Kingdom

Risk/Reward Managers
tel: +44 (020) 7562-9562
fax: +44 (020) 7628-5751
www.zyen.com

CL380 – Cyber Attack Exclusion Clause

1.1 Subject only to Clause 1.2 below, in no case shall this insurance cover loss damage liability or expense directly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any electronic system.

1.2 Where this Clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, Clause 1.1. Shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system computer software programme, or any electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile.

[Reference: Institute Cyber Attack Exclusion Clause 10/11/2003]

Page 19 in the report

Cyber-risk issues that challenge insurability and market development include the lack of actuarial data; difficulties in pricing; uncertainty around what is covered (wording and exclusions) and what the clients think they are buying; aggregation risk catastrophe models and the potential lack of adequate reinsurance capacity. You have to love this exclusion clause that excludes floods from a damaged dam control system, yet loops around to include "any electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile".

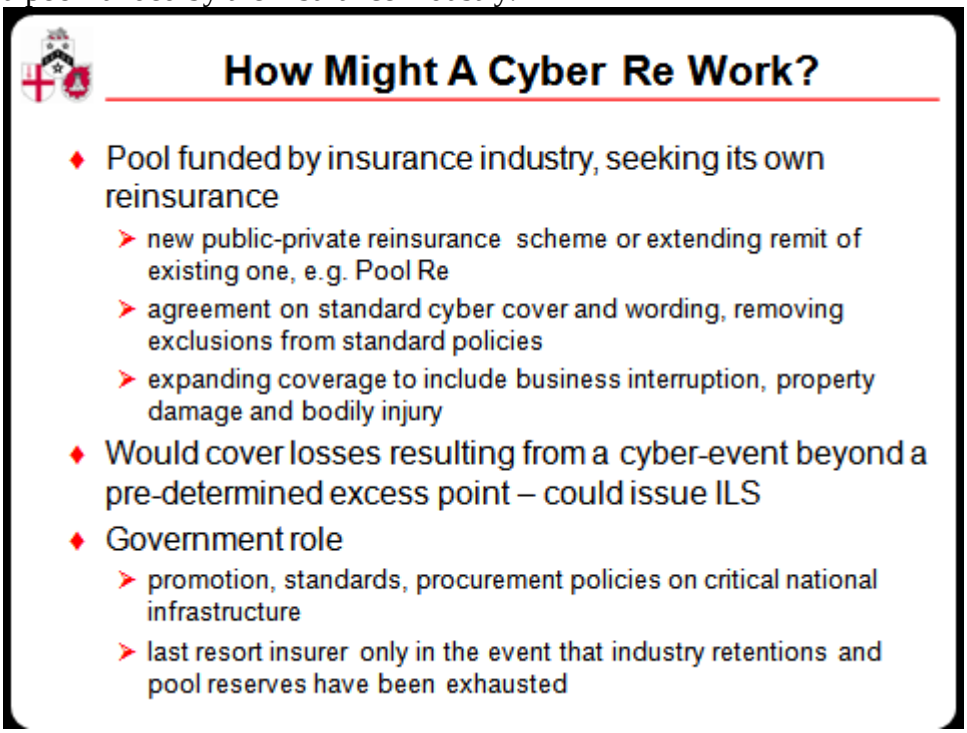
Mind The Gaps

	CRIME/ BANKERS BLANKET BOND	GENERAL LIABILITY	KIDNAP AND RANSOM	PROFESSIONAL LIABILITY	PROPERTY/ BUSINESS INTERRUPTION
FIRST PARTY CYBER LOSSES					
Network Interruption due to:					
» Computer Crime	■				
» Employee Sabotage	■				
» Operational Errors and Administrative Mistakes					
» Cyber Terrorism					
Restoration, Recollection, Recreation of Digital Assets due to:					
» Computer Crime	■				
» Employee Sabotage	■				
» Operational Errors and Administrative Mistakes					
» Accidental Damage to Hardware					
Cyber Extortion			■		
DATA PRIVACY AND SECURITY THIRD PARTY LOSSES					
Breach of Sensitive Third Party Information	■			■	
Data Breach Caused by a Third Party Outsourcer				■	
Corruption of Third Party Data by Malicious Code				■	
Distributed Denial of Service or Malicious Code Delivered via your Network				■	
Corruption or Deletion of Third Party Data				■	
Lost/Stolen Laptop or Hardware Containing Sensitive Third Party Data				■	
Data Breach due to a Security Breach				■	
Intellectual Property Infringement, Plagiarism and Defamation		■		■	
DATA PRIVACY AND SECURITY FIRST PARTY LOSSES					
Data Protection Fines and Penalties					
Data Protection Investigation and Defence Expenses					
Public Relations Costs					
Data Protection Legal Expenses					
Data Breach Notification Expenses					
Credit/Identity Theft Monitoring Expenses					

[Source: Willis, 2014 (selection for emphasis)]

It seems likely that cyber insurance will evolve to be a new class of insurance rather than an extension to existing policies. I would deem cyber risks to be under control when I can buy normal insurance after I've done what an insurer tells me I need to do to buy protection, just as I can buy home insurance against burglary or fire risks when I've done what's required.

One suggestion for government action is to speed development of the cyber insurance market by pushing for more rapid development of cyber reinsurance, helping insurers to grow much more swiftly. A public private cyber catastrophe reinsurance scheme could help secure cyber prosperity in the UK by helping insurers insure themselves to insure others. The scheme would provide cover to a group of insurers above a catastrophic loss threshold, in effect a pool funded by the insurance industry.



To start with, a Cyber Re (reinsurance) pool or club would help the insurance industry fund extreme losses. With a functioning cyber insurance market, the UK cyber market would be much more attractive to IT businesses such as financial exchanges and large internet firms. Such a Cyber Re could also help develop:

- more standardised wordings linking cyber catastrophe to the policies members write, and more standardised data collection for analytical purposes;
- proof-of-worth for ICT security and risk management standards.
- cyber catastrophe linked securities.

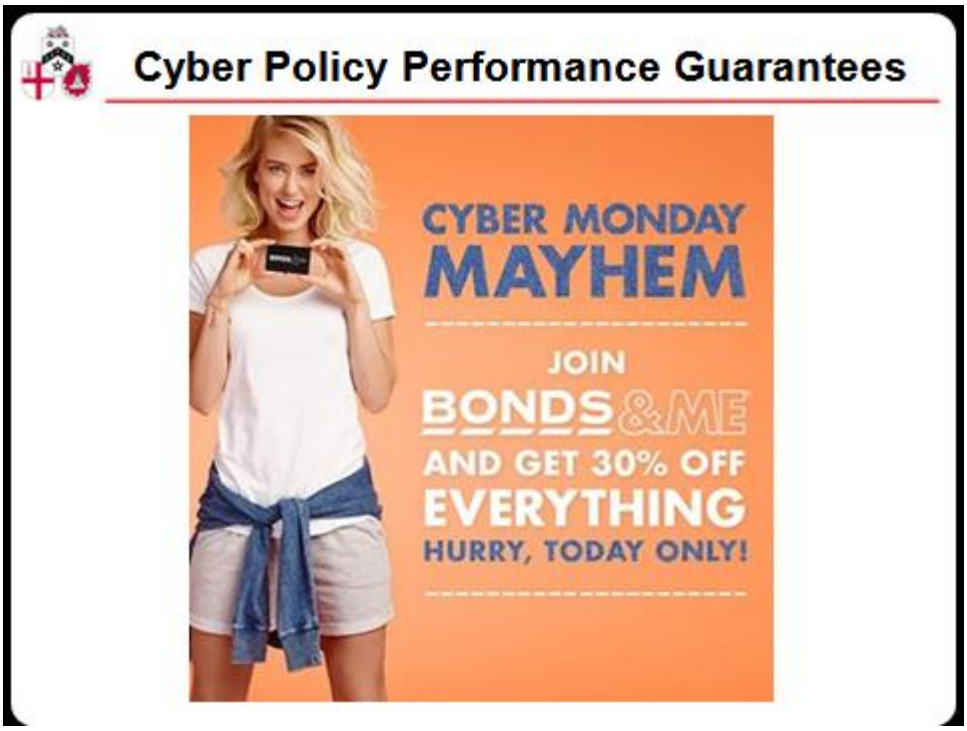
The UK government's role would be one of promotion and (possibly) a last resort insurer only in the event that industry retentions and the scheme's reserves have been exhausted. In all likelihood, the UK government would be a last resort insurer anyway but with a Cyber Re it would benefit from a buffer much deeper than today's. Government's role in a Cyber Re is small but crucial:

- insurance regulators should strongly encourage membership by insurers providing cyber cover;

90 Basinghall Street
London EC2V 5AY
United Kingdom
Risk/Reward Managers
tel: +44 (020) 7562-9562
fax: +44 (020) 7628-5751
www.zyen.com

- government and regulators should strongly encourage cyber insurance for essential services and critical national infrastructure including financial services, utilities, media, and incorporate cyber insurance in government;
- government oversight could help the issuance of cyber catastrophe linked bonds.

Cyber Policy Performance Guarantees



Under our 'expanding frontiers' intervention governments find it hard to prove that they are committed to policies. One approach to proving commitment on inflation has been to issue bonds that are linked to inflation targets. The first time principal and interest on a bond were linked to the price of a basket of goods was in 1780 by the State of Massachusetts. The Massachusetts basket included corn, beef, wool and leather. But inflation-linked bonds were not commonly issued until the 1980's. Growth has, however, been strong. In 2009 inflation-linked bonds represented 9% of worldwide outstanding sovereign debt.

Policy performance bonds are bonds whose funds are for general expenditure on roads, hospitals and schools, but whose payment terms are tied to successful policy outcome. They are a simple extension linking to other targets. Previously at Gresham, we have explored a simple, almost subversive, proposal on climate change finance – index-linked carbon bonds. I think in a lecture examining cyber-prosperity through economics, it is interesting to note that a cyber policy performance guarantee could be useful, and interestingly link with the Cyber Re idea too.

It might work like this. The government issues a bond that would pay a rate of interest linked to the amount of cyber damage done in a year. The more damage the more interest. The less damage the less interest. Companies and insurers with major exposure would buy such bonds to hedge their cyber risk. Another approach might be a cyber catastrophe bond where the government pays interest, but the bond principal is forfeit, does not need to be

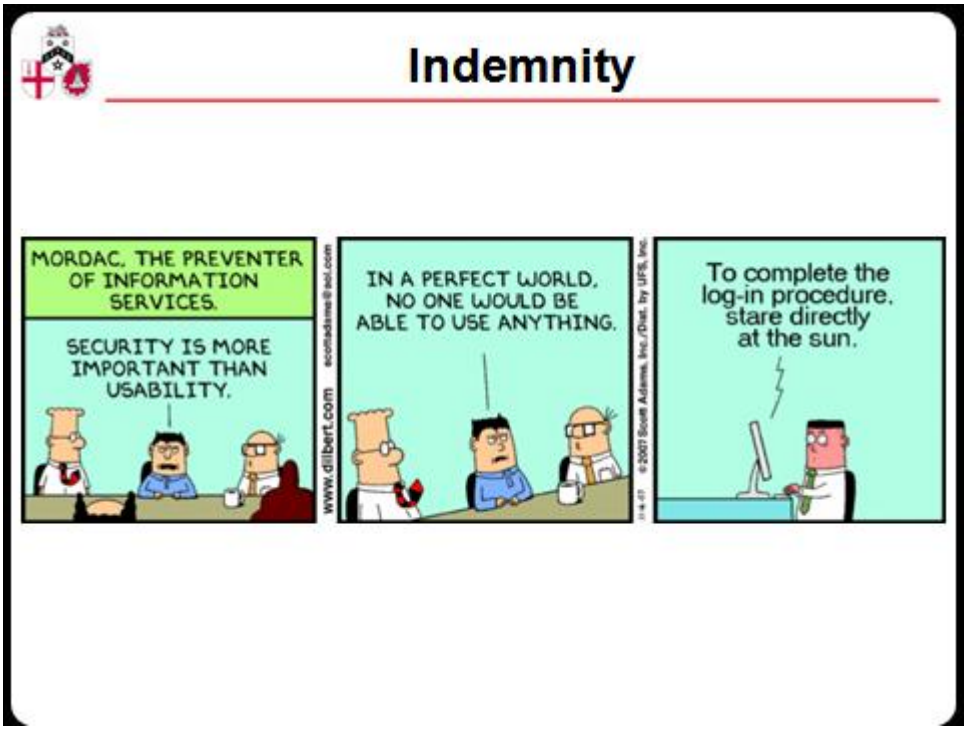
Risk/Reward Managers
90 Basinghall Street
London EC2V 5AY
United Kingdom
tel: +44 (020) 7562-9562
fax: +44 (020) 7628-5751
www.zyen.com

repaid, if say 20% of UK computers are out of action for more than 24 hours. Such financial structures may seem far-fetched, but are getting increasing attention as the webs between government and private finance intertwine deeper and tighter.

There are many areas worthy of deeper technical research from new cryptographic techniques to mutual distributed ledgers (aka blockchain technology), artificial intelligence defences, and quantum computers. To tackle our 13th intervention, fiat currency, please note that HM Treasury values defence, tax inspectors, and courts because they heighten faith in the persistence of the tax system and thus the fiat currency on which public and private economics in the UK depend. With the Bank of England actively examining a UK cryptocurrency, how much more important may it be for us work even harder on cyber security for cyber prosperity? If we move to a national cryptocurrency, our entire fiat currency would become a cyber policy performance guarantee.

One of the big cyber problems today is that even if I take all the advice of consultants and governments, no one backs up their advice with an indemnity. Indemnities are the real seal of proper advice, putting money where their consultant's mouths are. Insurance provides indemnities and forces advisors to prove their value, thus helping the entire economy learn how to manage risk.

Economic Over-Use?



As the slide above points out, the current situation is untenable. Users are not the enemy. Passwords have reached their limits. The internet has moved from research tool to utility, so sadly us old-timers needs to accept the need to move forward. But moving forward requires change on all sides that recognises the very economic honeypots that make investing in cyber-crime so attractive equally need economic solutions.

So, am I guilty of encouraging yet more innovation in government finance, an area already so full of inventive tricks that we have no idea if we can meet our pension or health obligations? We could point to the debacle of Private Finance Initiative and Public Private Partnerships as an example of government financial innovation gone mad, a government version of collateralised debt obligations. Perhaps, but I feel that we need to understand all the ways we can use government finance before we act, and this taxonomy of 12 ways, plus the monetary system itself, may help us to use government finance more wisely.

Economic success strains many of the original intentions behind the internet community and the original culture of the web continues to break down as real life intrudes. Perhaps foremost amongst the internet's founders' *sotto voce* intentions was serendipity. The journalist Aleks Krotoski says that our generation wanted a world of serendipity, meeting and exchanging virtually with strangers. In the morning a Nobel laureate could answer a question I posed, while in the afternoon a woman working in the fields of India could chat with me about local weather and her crops.

The founders of the web had ideals, principles, and emotions. The internet was supposed to establish relationships and create communities. These relationships were meant to be about sharing and co-creating information. As people developed information together there would emerge positive feedback and increasing communal trust. People like us would bring more people onto the internet and the world would become more like us as we all learned together. Without quite claiming the internet culture is broken, simply 'finding' or 'buying' things undermines the founders' ethos.

We have an internet that more and more fully reflects us – lovers and dreamers, police and thieves, politicians and journalists, philosophers and businesspeople. Functionality has often had a negative trade-off with serendipity. But not a complete trade-off. The more people realise they are living in a digital public realm the more it affects their decisions about what they choose to do and who they become. I think Aleks has a point when she wonders if it might be a good thing if we stop getting exactly what we want on the internet and instead seek to inject more serendipity, more randomness into our encounters. But of course that very serendipity creates more risk. What a conundrum.

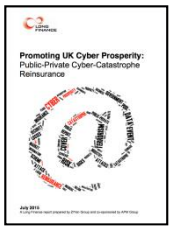
Risk/Reward Managers
90 Basinghall Street
London EC2V 5AY
United Kingdom
tel: +44 (020) 7562-9562
fax: +44 (020) 7628-5751
www.zyen.com


Promoting UK Cyber-Prosperity Through Economics
Thank you!
LONG FINANCE
www.zyen.com
THEOLOGICAL BARGAINS
"Get a detailed grip on the big picture."
Chao Kli Ning

Thank you.

Further Surfing

- Michael Mainelli, Gresham College - "Risk, Equality and Opportunity: The Roles for Government Finance" – London, England (4 December 2012)

	**Promoting UK Cyber Prosperity: Public-Private Cyber catastrophe Reinsurance**	Michael Mainelli, Chiara von Gunten and Mark Duff, Z/Yen Group Limited	2015	Long Finance report prepared by Z/Yen Group co-sponsored by APM Group (July 2015), 50 pages

- Public-Private Cyber catastrophe Reinsurance - http://www.longfinance.net/lf-research.html?id=780
- Policy Performance Bonds - http://www.longfinance.net/lf-research.html?id=778

Previously at Gresham College

All past lectures –
http://www.gresham.ac.uk/lectures-and-events/past?keys=&field_speakers_nid=1212&field_lecture_date%5Bvalue%5D%5Byear%5D=&field_lecture_date%5Bvalue%5D%5Bmonth%5D=&term_node_tid_depth=All

Thanks

With much appreciation for the many people who have discussed several of these topics with me, may I thank in particular Bill Joseph for teaching computing in the early 1970s, the APM Group for their support of the report, Julian Enoizi of Pool Re for being open to the ideas of cyber reinsurance, Mike St John Green and Adrian Leppard for providing a sensible government perspective, but most importantly the report's co-authors Chiara von Gunten and Mark Duff for being such great people with whom to work.

90 Basinghall Street
London EC2V 5AY
United Kingdom

Risk/Reward Managers
tel: +44 (020) 7562-9562
fax: +44 (020) 7628-5751
www.zyen.com