

Mitsui Sumitomo at Lloyd's

Excellence in all we do

**MSIUL Risk Management Seminar
22nd September 2011**

Cyber Security - The emerging risk



Jonathan Poole
MSIUL Claims Director

Agenda

- Definition of Cyber risk
- Risk identification measures
- Keys to Cyber risk management
- The Cyber insurance market
- Q&A



Everyone is talking about it!!



MSIG

SONY
hacked.again



Data damage and destruction beyond the naked eye



"It's long been said that the revolutions in communications and information technology have given birth to a virtual world. But make no mistake; this world, cyberspace is a world that we depend on every single day. It's our hardware and our software, our desktops and laptops and cell phones and Blackberries that have been woven into every aspect of our lives.

It's the broadband networks beneath us and the wireless signals around us, the local networks in our schools and hospitals and businesses and the massive grids that power our nation. It's the classified military and intelligence networks that keep us safe and the world Wide Web that has made us more interconnected than at any time in human history.

So, cyberspace is real and so are the risks that come with it. It's the great irony of our Information Age – the very technologies that empower us to create and build also empower those who would disrupt and destroy. And the paradox, seen and unseen is something that we experience every day"

President Obama, May 2009



Cyber crime headlines



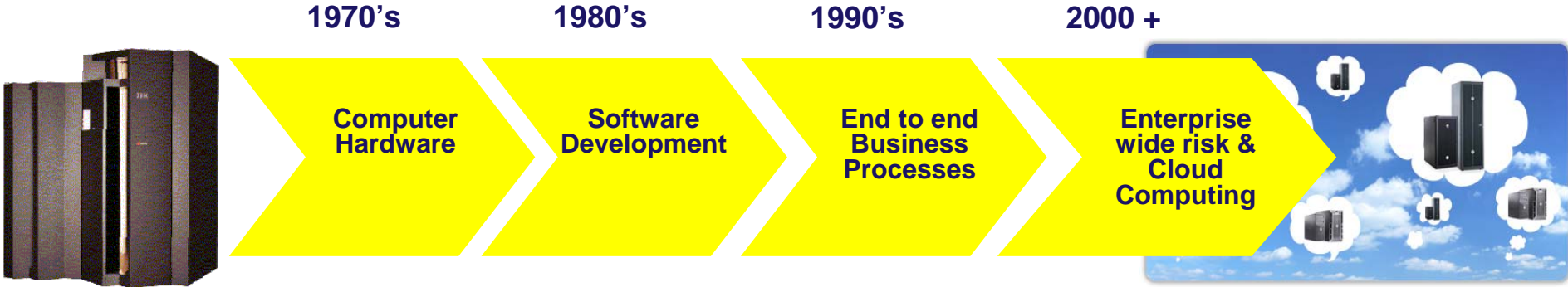
- Statistics make grim reading
 - Cyber crime costs the UK economy alone £27bn a year*
 - The proceeds from worldwide cyber crime exceed those from illegal drugs
 - Intellectual property theft or industrial espionage costs UK businesses £9bn a year*
- What are you doing to protect your balance sheet?
 - What are your IT assets and what are they worth?
 - How reliant are you on IT as an enabler of your business?
 - Does the business understand the value of IT and IT the value of the business?

* Source - Detrica

What are Cyber risks?



IT evolution



Definition of Cyber risk

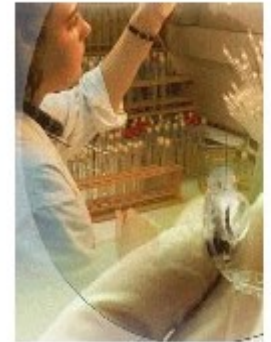


Cyber risk refers to the potential losses and liabilities arising out of e-commerce;

- Computer networks (Internal exposure)
- The internet (external exposure)

Cyber risks can be broadly categorised into;

- Content risk
- Technical risks



Content risks



Technical risks

- Unauthorised access
- Viruses, malicious codes or Trojan horses
- Cyber extortion
- E-theft or destruction
- Deliberate overloading of web servers



Objectives of Cyber risk

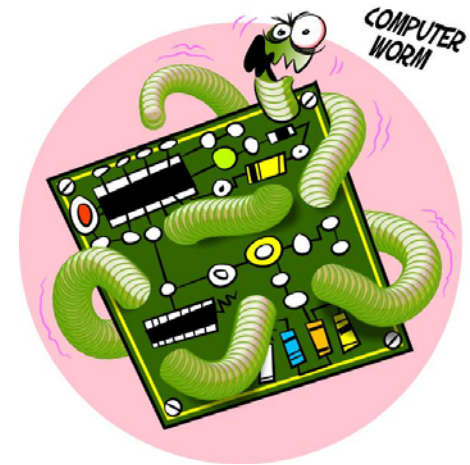
- Financial theft
- Identify theft
- Fraud
- Extortion
- Revenge
- Pride
- Fun



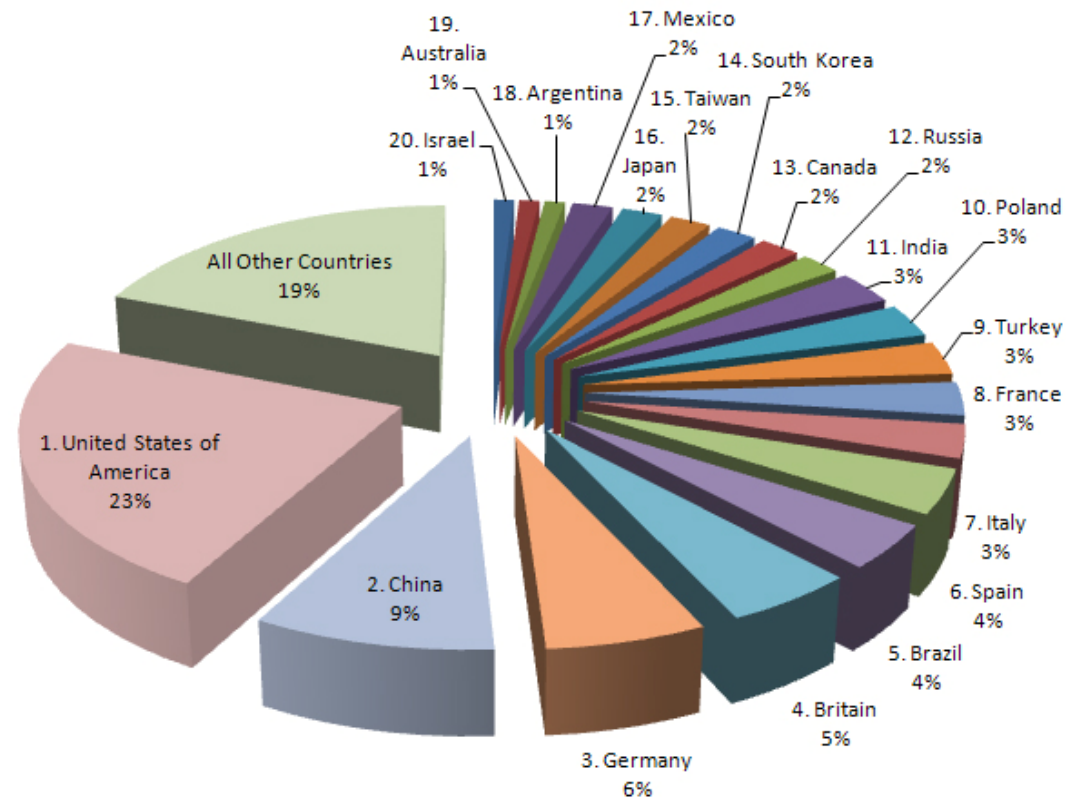
Cyber risk tools



Image courtesy of: Tech Tips.com



Geographic distribution of Cyber crime

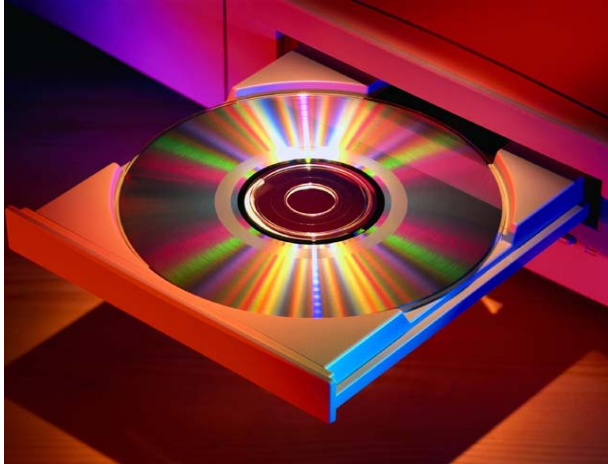
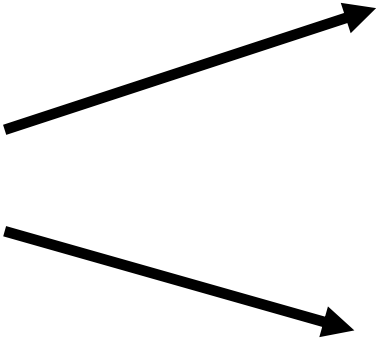


Cybercrime: Top 20 Countries

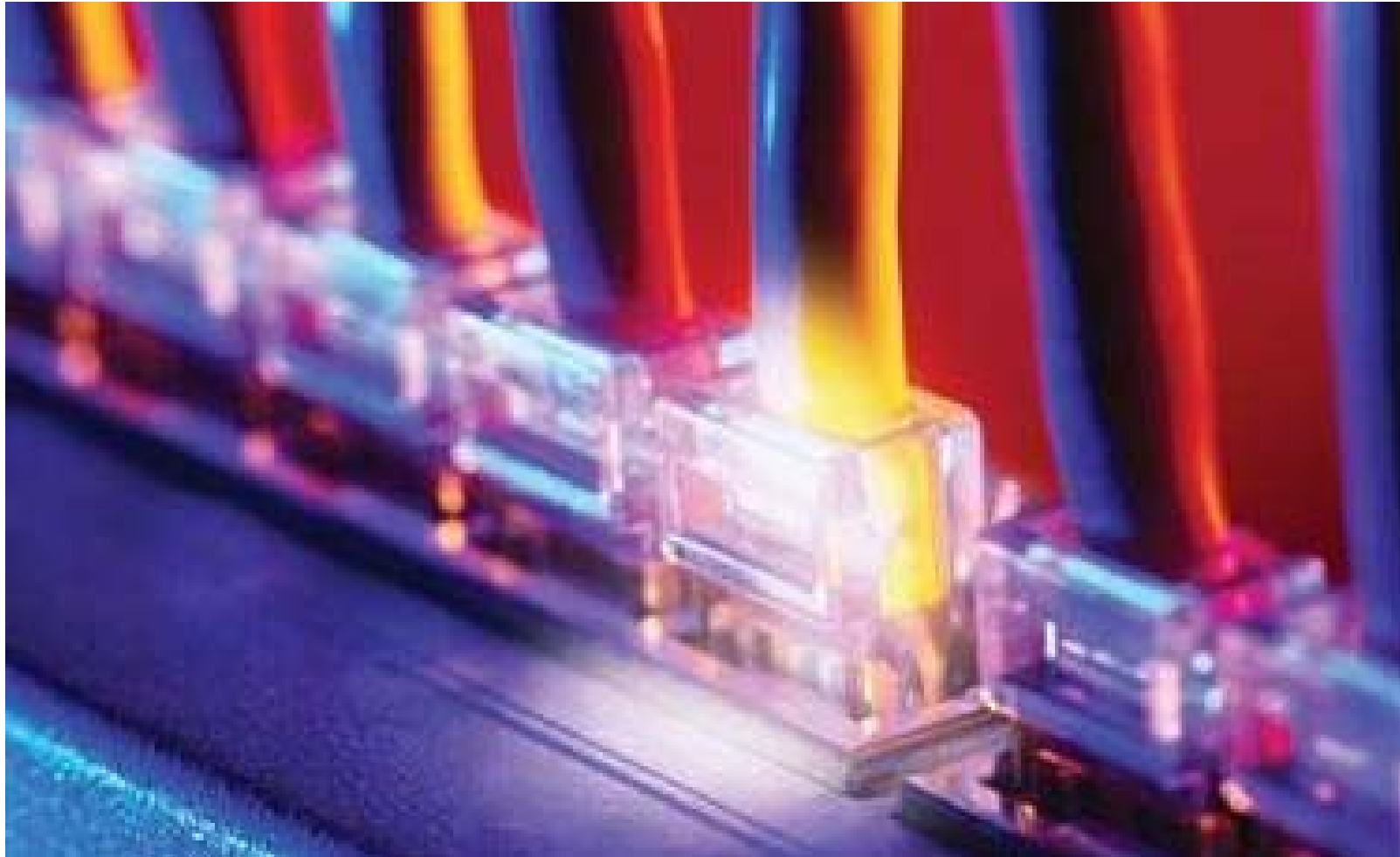
Key assets are changing...



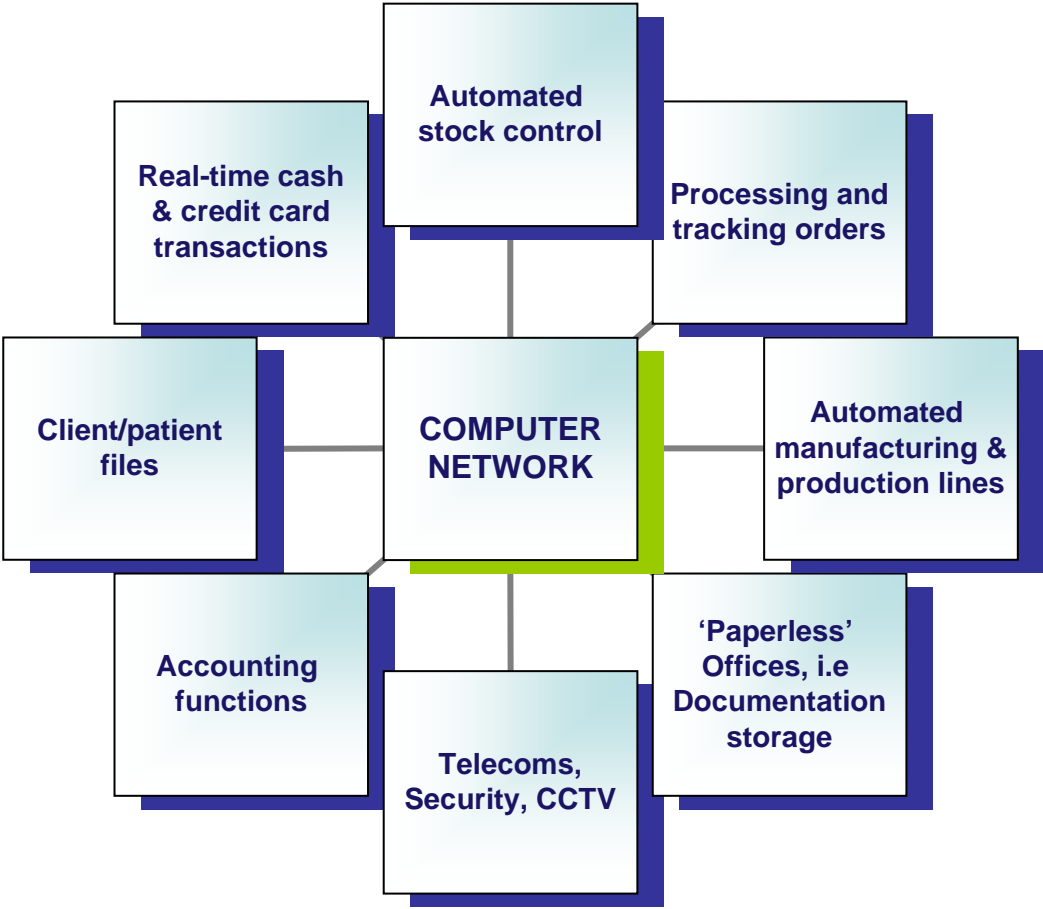
MSIG



Network functions



Computer network functions



Enterprise risk management



Risk identification

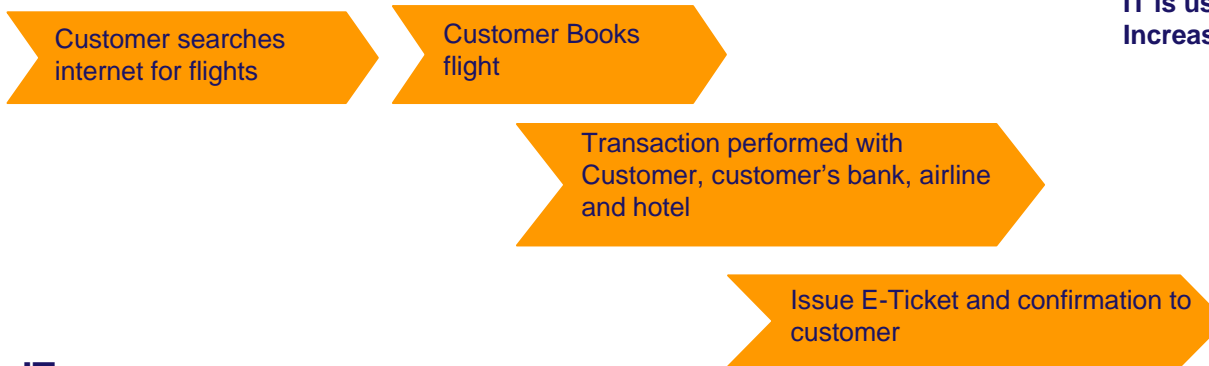
- Real-time business process and increased e-commerce has increased scope for gains in productivity and efficiency, but have created a dependency which has brought about increased risk.
- The increased reliance on connectivity of IT networks is a systemic risk.
- Some companies operate purely as e-commerce organisations, creating a major risk in terms of internet connectivity.
- Business critical networks



Does business drive IT or IT drive the business?

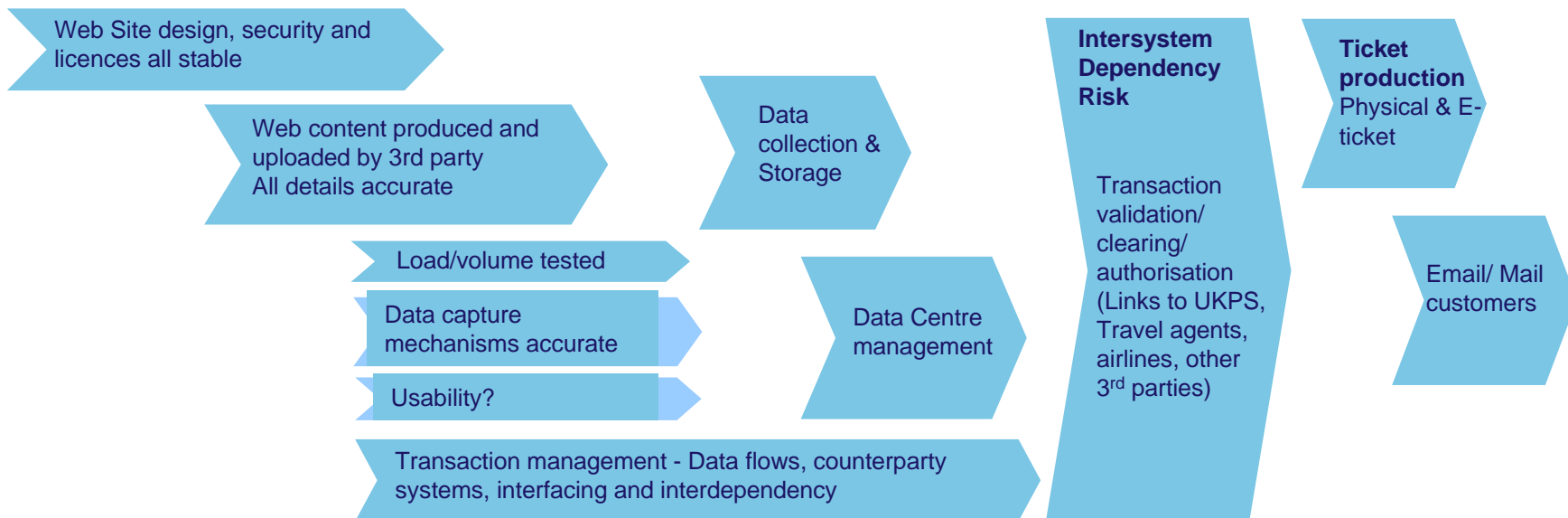


Business process



IT is used as the primary business enabler:
Increase profits – reduce costs

IT process



Cyber Risk Management



- Comprehensive Cyber risk analysis
 - What is the internet being used for?
 - What security measures are in place?
 - Is internal audit already involved in testing security measures?
 - Is security tested by an outside party?
 - Are there strong internal controls around Cyber risk management?
- Detailed business impact analysis
 - Quantify the potential loss to the company, including aggregate exposure values.
- Business Interruption and Disaster Recovery Planning
- Training and awareness
- Governance and Board level ownership

First party loss exposures



- First party claims often relate to losses arising from e-commerce or internet related activities;
 - Damage to intangible property, such as software programmes and electronic data
 - Business Interruption resulting from damage to intangible property
 - Theft of proprietary information
- Cyber perils giving rise to first party losses are as follows;
 - Hackers (external and internal)
 - Viruses
 - Extortion
 - Programming errors
 - Network or systems failures arising from power surges

Third party liabilities



- Key exposure is a Company's liability for sustained losses arising out of the use of e-commerce or internet related activities. Examples include;
 - Damage to third party property, i.e. software, data and/or financial
 - Intellectual property infringements
 - Defamation, libel and slander
 - Invasion of privacy
 - Unfair competition or false/misleading advertising
 - Unauthorised use of confidential information

Cyber insurance market



- Cyber policies do not fit neatly within definitions and exclusions associated with traditional insurance policies.
- There is not always a trigger, giving rise to an insured event, i.e. direct physical loss or damage under a Property policy.
- Most General Liability policies do not cover economic loss or professional services, precluding most cyber risk damages.
- Theft of intellectual property is not addressed by many policies
- Errors or omissions policies often contain security breach exclusions.
- Many insurance policies have geographical limitations; the internet does not.
- There is little historical data and risks are often poorly defined and lacking in definition

Cyber insurance market



- Increasingly, cyber specific policies are emerging.
- Professional Liability insurers are willing to consider intellectual property infringements when they have a deep understanding of the insured's culture and risk awareness
- A limited market for non physical damage BI now exists
- Coverage within crime policies now often includes computer fraud
- Insurers will need to see evidence of proactive cyber risk management prior to granting capacity.

Conclusion

- Cyber risks present new and different challenges which can effect a Company's financial stability.
- Increasing media interest in computer crime has highlighted that the first lines of technological defence are no longer impenetrable.
- Network security breaches can expose companies to class action law suits, significant Business Interruption and irreversible damage to the corporate brand.
- Liabilities will continue to grow and evolve as the risk emerges.
- Insurance for cyber risk is continuing to evolve, as more companies need to develop a Cyber risk management strategy and transfer elements of that risk from their own balance sheet.



The future...



MSIG

