CHUBB

Cyber & technology risk – how to manage a Chimera?

Karachi, April 2017

Agenda

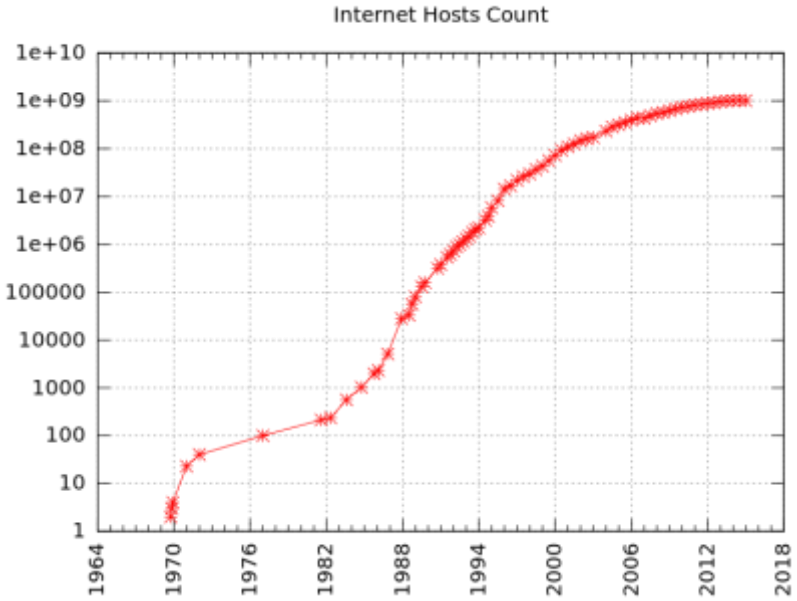
- Introduction
- Cyber risk: the modern chimera
- What is cyber risk?
  - Sources
  - 1st & 3rd party exposures
  - Claims examples
- How can businesses protect themselves
- Insurance solutions
  - Challenges for insurers
  - How the market has developed
  - The Chubb ERM approach
- Summary & questions

Who are Chubb?

- The world's largest publicly traded property and casualty (P&C) insurer.
- Insurance is our only business.
- Well balanced by product and customer:
  - A global leader in traditional and specialty P&C coverage for industrial commercial and mid-market companies
  - A leading commercial lines insurer in the U.S. and the largest financial lines writer globally
  - The leader in U.S. high net worth personal lines and a large personal lines provider globally
  - A global leader in personal accident and supplemental health insurance
  - A P&C reinsurer
  - An international life insurer focused on Asia
- Chubb Limited, the parent company of Chubb, is listed on the New York Stock Exchange (NYSE:CB) and is a component of the S&P 500 index.
- Exceptional financial strength, managing risk conservatively in both underwriting and investing.
- Core operating insurance companies are rated "AA" for financial strength by S&P and "A++" by A.M. Best.
- A truly global company, with local operations in 54 countries and territories.
- **MULTINATIONAL CYBER CAPABILITY:** Over 50 countries worldwide, increasing regularly as we roll out our Cyber ERM policy.

Growth of the internet

"When I took office, only high energy physicists had ever heard of what is called the World Wide Web… Now even my cat has it's own page."
- Bill Clinton



Number of internet hosts: 1969-2012

Source: Internet Systems Consortium

Year	Users (millions)	% of Global Population
1995	16	0.40%
2000	361	5.80%
2005	1018	15.70%
2010	1971	28.80%
2015	3366	46.40%
2016	3696	49.50%
Mar-17	3732	49.60%

Source: IDC, CI Almanac, Nua Ltd., Internet World Stats

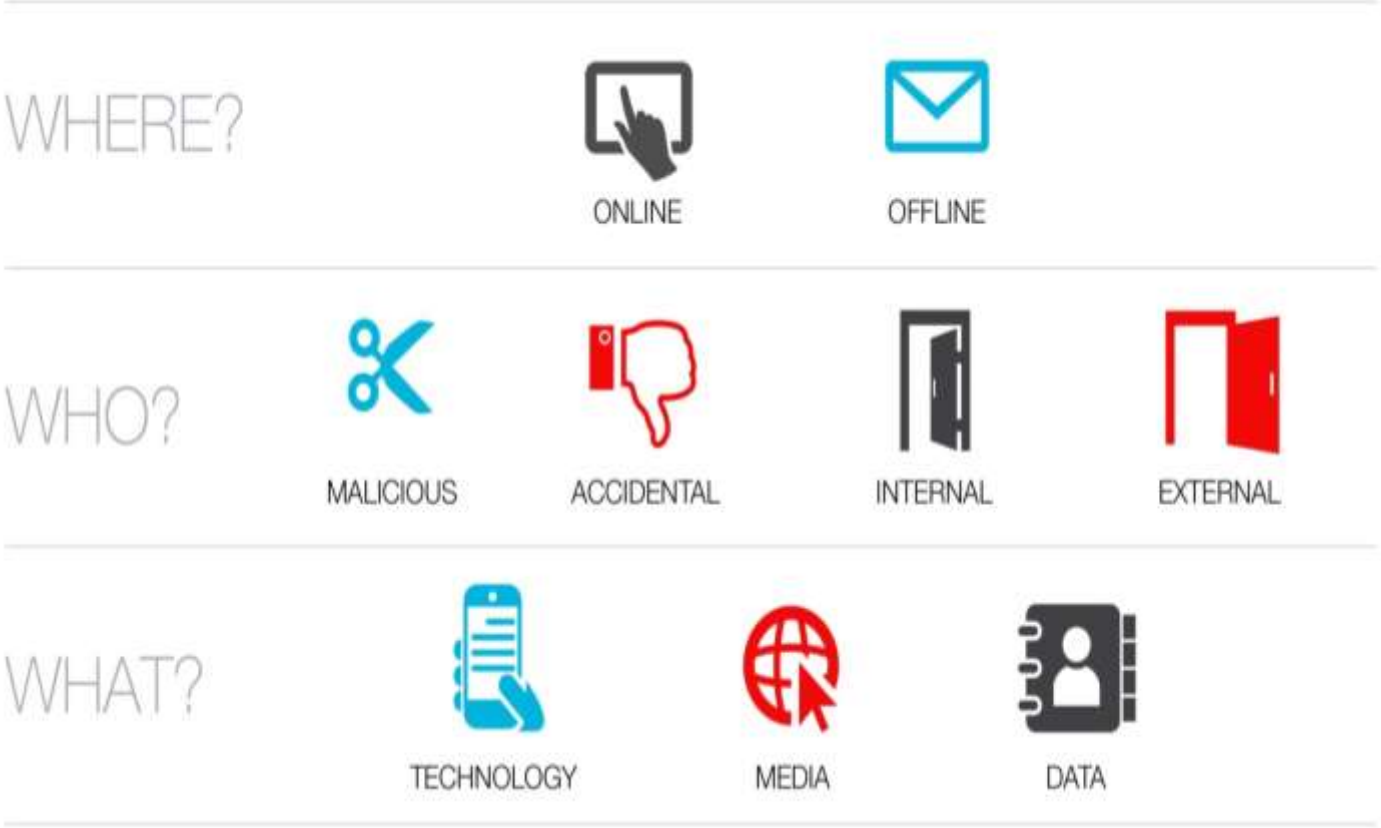
"In order for insurance to remain relevant in society, you can't simply hold on to the past.... Perils are emerging as society matures...as economy digitizes, as society digitizes, there are more exposures that are going to emerge. Cyber risk is one of them."

— Evan Greenberg, Chubb Chairman and CEO

What is Cyber Risk?
A brief visit to Ancient Greece: the Chimera

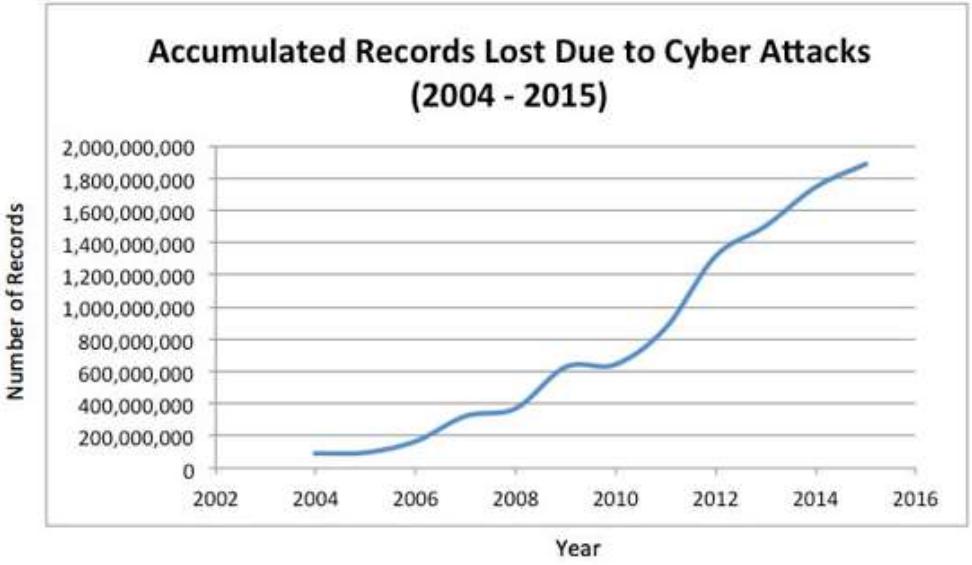
"a creature fearful, great, swift-footed and strong, who had three heads, breathing forth a fearful blast of blazing fire."

What is Cyber Risk?



Cyber attacks

92% of European businesses suffered a cyber breach in the past 5 years - Lloyd's (Sept 2016)

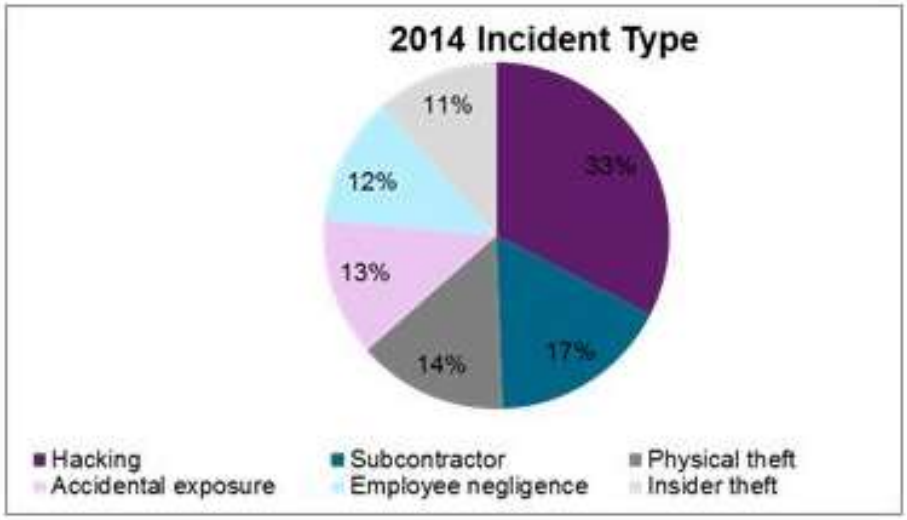


The steadily increasing number of records lost to cyber attacks 2004–15.
(Data Source: Insurance Information Institute)

Future drivers:

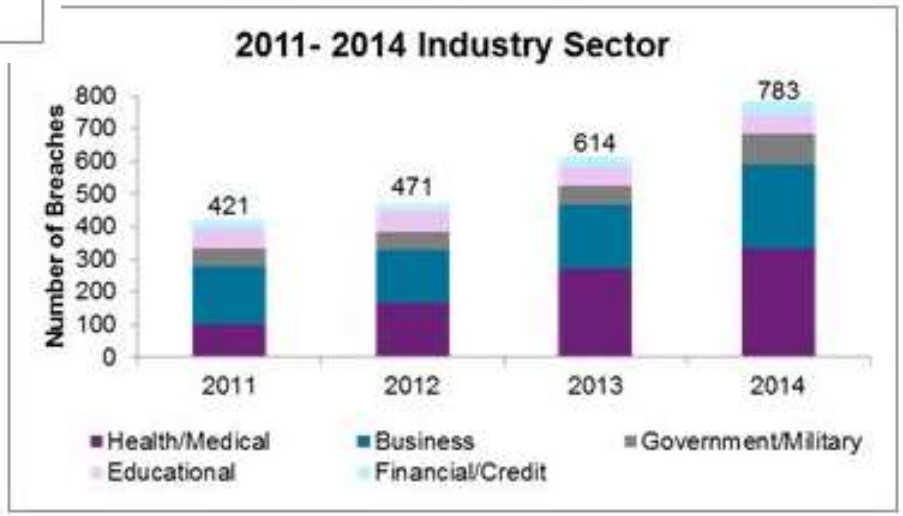
- Social media use
- The internet of things
- The industrial internet

Types and targets of cyber incidents



Scale of loss is influenced by incident type, but perhaps the most important consideration is the attacker's goal – from simply showing off to full-blown extortion

Different industry sectors have different cyber concerns: data loss, privacy, downtime, reputational impacts, regulatory responsibilities



Source Property 360

What are the potential outcomes?

1st Party Risks

- Crisis Management Expense
- Recovery Costs and Extra Expenses
- Lost Income

3rd Party Risks

- Legal and Regulatory Defence Costs
- Fines and Penalties
- Legal Liability

Claims examples

Scenario 1: Employee Error	Potential Impact	
An HR recruiter for a healthcare organisation accidentally attached the wrong file when sending an email to four job applicants. The file included HR demographic data consisting of 43,000 former employee names, addresses, and national ID numbers. The insured telephoned the Chubb Incident Response Hotline for assistance and an incident response manager was assigned. Legal services were brought in to manage regulatory implications.	**Privacy Liability** - mismanagement of personal and/ or corporate confidential information, violation of company privacy policy. - Defence expenses arising from regulatory investigation. - Defence and settlement costs for claims employees that had identity stolen **Incident Response Expenses** - Incident response manager fees - Notification to affected individuals - Identity theft monitoring services for affected individuals - Legal consultation fees	£55,000 £100,000 £5,000 £3,000 £13,000 £10,000
Takeaways As innocent as it may seem, human error can be very costly, and it occurs more frequently than expected. It's important to understand that cyber is not only related to technological incidents. Many of the claims we see stem from very simple mistakes.		**Total Cost: £186,000**

Claims examples

Scenario 2: Denial of Service Attack	Potential Impact	
The data centre which hosted an online retail company's website became the target of a distributed denial of service attack. The attack, which utilised hacked internet of things devices, flooded the data centre's network with so much traffic that their network failed. This made the online retail company's website inaccessible for a period of six hours before backup systems were able to restore 100% functionality. The insured in this scenario is the online retailer. After telephoning the Chubb Incident Response Hotline, an incident response manager was assigned.	**Recovery Costs** - Increased cost of working required to get website functioning properly - Costs to subcontract with external service provider **Business Interruption** - Lost sales and revenue from website downtime **Incident Response Expenses** - IT forensics firm - Legal consultation fees - Incident response manager fees	 £9,000 £12,000 £95,000 £12,000 £10,000 £6,000
Takeaways Distributed Denial of Service (DDoS) attacks are becoming more powerful as the use of easily hacked internet of things devices increases. To minimise impact of a scenario like this one, it is important to build a business continuity plan that ensures critical business applications, systems, and activities do not rely on only one critical IT provider. Chubb's incident response managers and vendors are experienced in dealing with DDoS attacks and will assist in getting your business back on track as soon as possible.		**Total Cost: £144,000**

Claims examples

Scenario 3: Ransomware Attack	Potential Impact	
An employee of a car components manufacturing company clicked on a malicious link in an email and malware was downloaded onto the company server, encrypting all information. A message appeared on the employee's computer demanding £10,000 to be paid by Bitcoin in the next 48 hours in exchange for the decryption key. The company telephoned the Chubb Incident Response Hotline for assistance. The assigned incident response manager brought in IT forensic investigators to assess the validity of threat and to determine whether the company could avoid paying the ransom.	**Network Security Liability** - failure of insured's network security in defending against computer malicious acts	See Incident Response (Below)
	Cyber Extortion - costs associated with addressing extortion threats to release information or malicious code unless extortion monies were paid	
	- Information technology consultant fees to assess backup capabilities	£14,000
	Incident Response Expenses	
	- Forensic investigation costs to locate malware, analyse impact, ensure containment, and calculate extent of loss	£18,000
	- Legal consultation fees	£7,000
	- Incident Response Manager fees	£6,000
	Data Asset Loss - costs associated with replacing lost or corrupted data	£15,000
Takeaways While the Bitcoin demand was less than the costs incurred under the insurance policy, it is encouraged by both Europol and the FBI that cyber ransoms should not be paid. Not only does paying the ransom perpetuate criminal activity, but it also highlights a company's lack of effective and responsible backup procedures. Backups should be stored off-site and off-network. Chubb understands that there are certain scenarios when paying a ransom is the last but best option, which is why Chubb's incident response vendors are equipped with Bitcoin wallet capability if necessary.		**Total Cost: £60,000**

CHU

The Business Challenge

It's not a matter of if,

It's not a matter of when,

It's a matter of *how*.

How you **prepare** and **respond**.

10 Steps To Cyber Security

CESG

Defining and communicating your Board's Information Risk Management Regime is central to your organisation's overall cyber security strategy. CESG recommend you review this regime - together with the nine associated security areas described below - in order to protect your business against the majority of cyber threats.

User Education and Awareness

Produce user security policies covering acceptable and secure use of the organisation's systems. Establish a staff training programme. Maintain user awareness of the cyber risks.

Home and Mobile Working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline build to all devices. Protect data both in transit and at rest.

Network Security

Protect your networks against external and internal attack. Manage the network perimeter. Filter out unauthorised access and malicious content. Monitor and test security controls.

Establish an effective governance structure and determine your risk appetite.

Information Risk Management Regime

Secure Configuration

Apply security patches and ensure that the secure configuration of all ICT systems is maintained. Create a system inventory and define a baseline build for all ICT devices.

Malware Protection

Produce relevant policy and establish anti-malware defences that are applicable and relevant to all business areas. Scan for malware across the organisation.

Maintain the Board's engagement with the cyber risk.

Produce supporting information risk management policies.

Removable Media Controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing on to the corporate system.

Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all ICT systems and networks. Analyse logs for unusual activity that could indicate an attack.

Managing User Privileges

Establish account management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident Management

Establish an incident response and disaster recover capability. Produce and test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.

Department for Business Innovation & Skills
CPNI Centre for the Protection of National Infrastructure
Cabinet Office

"The global cyber insurance market, dominated by North America, is expected to generate $14 billion in gross premiums by 2022, growing at a compound annual growth rate of nearly 28% as insurers expand coverage to other regions…"

- Business Insurance / Allied Market Research

Global cyber insurance market size

Source: PwC Global State of Information Security Survey 2016

CHUBB

Chubb Cyber ERM

Measurement, Management, Crisis Response, Coverage

Chubb value proposition

- Specialized Underwriting Expertise
  - Dedicated Technology Underwriters
  - Deep Industry Knowledge
- Customized Products
- Account view and solutions including Property GL E&O/Cyber
- Global Program Capabilities
- Claims and Loss Control Expertise

NB: Each market requires specific evaluation – risks, regulation and TP support capabilities all vary.

Cyber ERM Coverage

Incident Response	Supports all insuring agreements to efficiently mitigate any covered event.
Privacy Liability	Liability arising from the duty to maintain confidentiality of: - Personal information, or - Corporate information.
Network Security Liability	Liability arising from the duty to maintain network security for third parties.
Cyber Extortion	Cover for expenses and ransom (where insurable) - Multinational - Ability to Pay in Bitcoin

Media Liability	Cover for online media - Includes Social Media Websites
Data Loss	Cover for destruction, lockout, or corruption of data, including: - Power Surge or Failure - Accidental Events
Business Interruption	Costs and lost income due to the inability to access computer systems caused by: - Malicious Acts - Accidental Acts - Programming Error
Recovery Costs	Includes: - Costs to lease equipment, and - Increased labor costs

Thank you.

Questions?

Chubb. Insured.