INNOVACIÓN, TECNOLOGÍA Y SEGUROS

Sesiones Daños - Ponencia 4

Cyber Risks Business Impact

PRINCIPIA UNDERWRITING

26 CONVENCIÓN DE ASEGURADORES AMIS

Chris Newton
Principia Underwriting

19 de abril 2016

Principia Underwriting

- Specialist underwriting agency utilising Lloyd's of London capacity

- Suite of technology and media liability offerings, including cyber - network security, privacy liability, crisis management and non-physical business interruption

26 CONVENCIÓN DE ASEGURADORES AMIS

PRINCIPIA UNDERWRITING

What are cyber risks?

- Malicious software
- Hacking
- Malicious acts of employees
- Social engineering – spam, phishing, pharming
- Denial of service attacks
- Extortion
- Physical and non-physical business interruption

What are cyber risks?

- Reliance on computer-based infrastructure makes us more vulnerable to cyber attacks on computer systems, networks and data

- Targets for cyber criminals and hacktivists seeking personal data or running scams for information or financial reward

- We are reliant on the interconnectivity between computers, networks and the internet, made all the more vulnerable by cloud and mobile technologies.

What are cyber risks?

- We now have close to 25 billion connected IT devices such as PCs, servers, routers, industrial control systems, medical machinery and operational technology.

- The ‘Internet of Things’ now exists, a network of physical objects embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data

What are cyber risks?

This enables:

- manufacturers to track inventory and raw materials, manage supply chain logistics and control industrial processes
- retailers to track deliveries and use sensors for stock control and replenishment
- power generators use smart grids to manage supply and demand
- health care organizations use remote monitoring systems for medical conditions

What are cyber risks?

Data and operational systems also have a value to the unauthorised user.

The use of technology enables individuals and organizations to target those sources of data

- for criminal or politically motivated reasons, or
- in the case of hacktivists, simply as a means to beat the system.

Stolen data can be used for hacking purposes, theft, identity theft, cyber stalking, establishing fraudulent lines of credit or for monetizing via the dark web.

What is the value of this data to the criminal?

Recent Dell SecureWorks' report identified the latest price list for hacker goods and services:

- Banking credentials change hands for between 1 and 5 per cent of the account balances.
- American Express Cards fetch $30, towards the upper end of prices for plastic card credentials, which start at $7 and rise depending on the type of card and the amount of associated data offered for sale.
- Distributed denial of service attacks can be contracted for as low as $5 an hour, the same price as remote-access trojans.

What is the value of this data to the criminal?

- Angler exploit kits – a common hacking tool that's used to sling malware from compromised or hacker-controlled websites – are licensed from $100

- ATM skimming devices can be had for $400 or less

- Hacking a corporate email account costs $500 per mailbox, whereas a Gmail or Hotmail account costs $123

What is the value of this data to the criminal?

- A physical counterfeit French driver's license for $238 or German, US, Israeli, UK and international driver's licenses for about $173.

- European passports are on offer from $1,200

- The prices of identity documents have gone up while the cost of other items, particularly malware, has reduced

What is the value of this data to the criminal?

- Other items offered for sale include hacking tutorials, airline points and complete personal information dossiers (names, addresses, dates of birth, etc).

- These dossiers can be used for identity theft or other malicious purposes.

What is the value of this data to the criminal?

As a result, incidents of cyber crime or attack have the potential to cause major disruption and financial loss.

- In their most disruptive form, cyber attacks target the enterprise, government, military, or other infrastructural assets on a national and individual level.
- Targets range from countries' critical national infrastructure and financial system, to manufacturing, industrial and mining companies.

What is the value of this data to the criminal?

- More and more private and public sector organisations are capitalising on web, mobile and social media platforms to improve their performance and serve customers more effectively.
- As the use of online services increases, the scale, volume and sophistication of cyber threats (cyber warfare, cyber terrorism, cyber espionage and malicious hacking) are increasing.
- As people do more business online, criminals are developing ever more sophisticated ways to break into systems and steal information, take control of computers and defraud companies and individuals.

What is the value of this data to the criminal?

- It is estimated that nearly two thirds of employees steal proprietary corporate data when they quit or are fired

- Product designs, business plans, databases and marketing programmes all have a value to competitors

- Disgruntled staff may also deliberately sabotage a business by deleting records or planting computer programmes designed to destroy data at a preset time in the future

What is the value of this data to the criminal?

- Connecting industrial control and SCADA systems to the corporate IT network gives organisations access to improved management information and consequently a better understanding of what is happening across the business.

- This degree of connectivity means that industrial control systems are exposed to cyber security threats similar to those faced by corporate networks.

What is the target?

- Intellectual property – corporate confidential information, merger and acquisition data, patents, industrial process and trade secrets, operational data, trading results

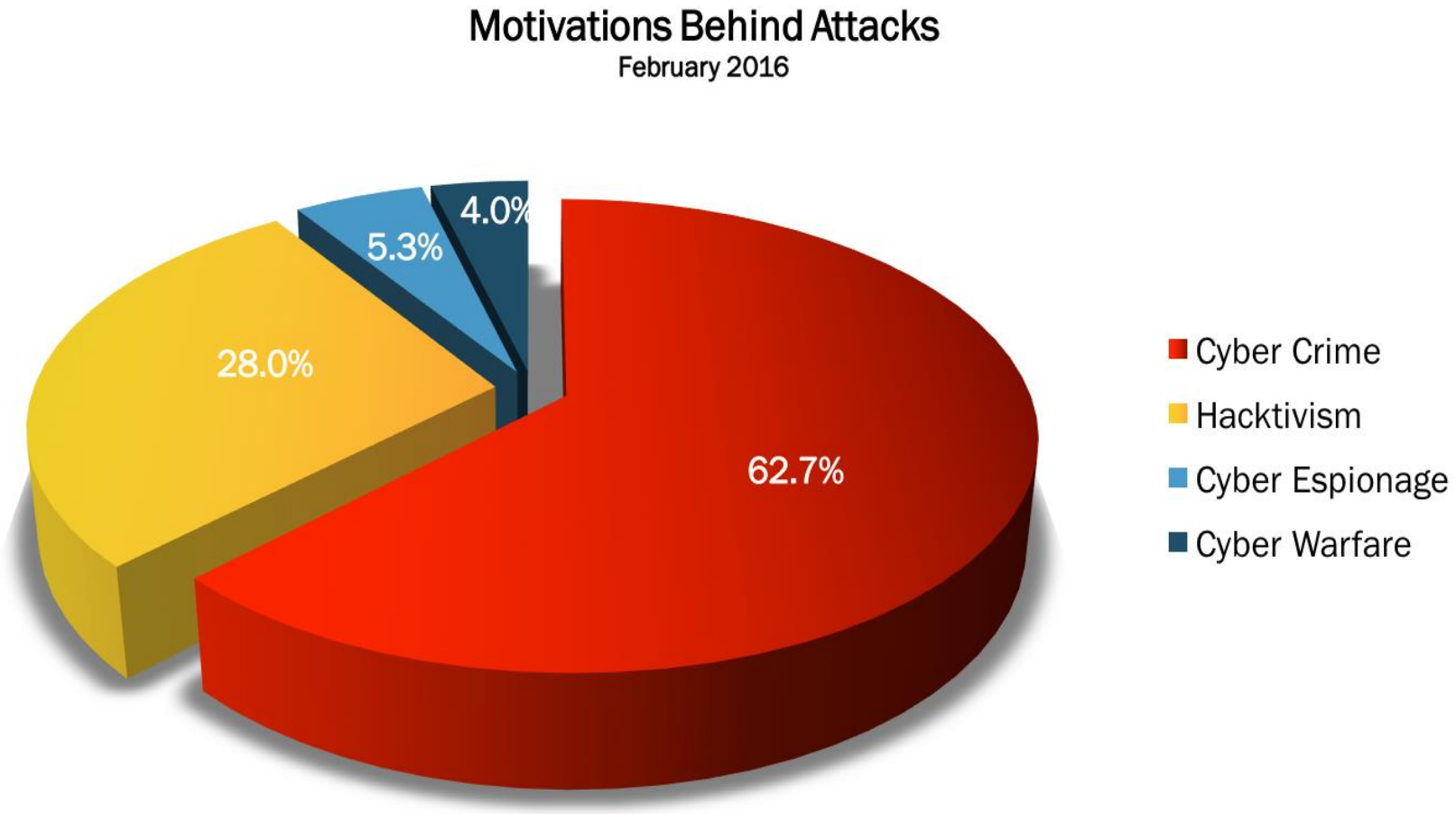
- Personal sensitive data – financial information, bank accounts, social security numbers, drivers license, payment card data

- Operational systems – industrial controls, manufacturing lines, supply chain, remote process control

Perpetrators

- Motivation
- Technical capability
- Infrastructure
- Market

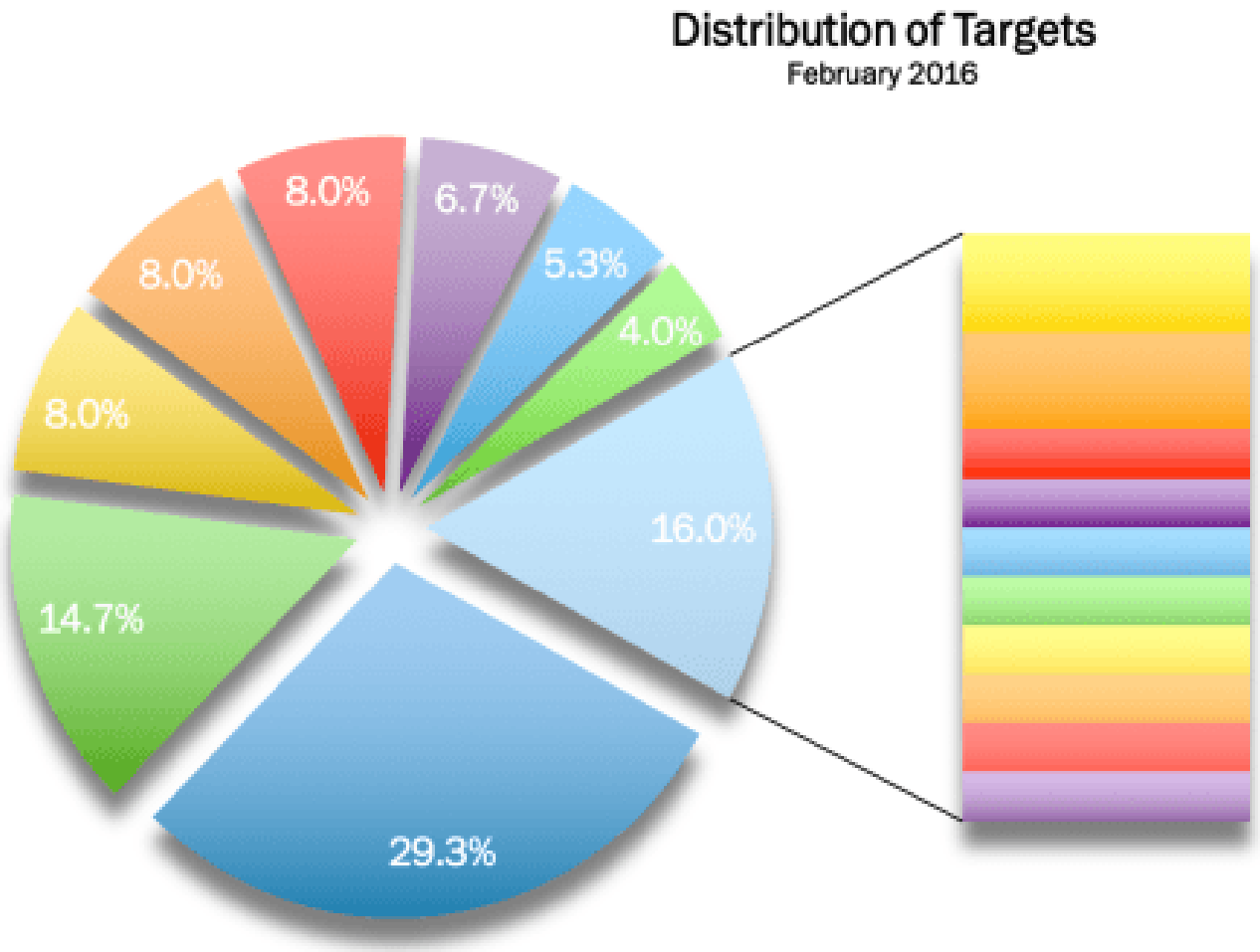
Motivation Behinds Attacks



26 CONVENCIÓN DE ASEGURADORES AMIS

PRINCIPIA UNDERWRITING

Motivation Behinds Attacks



26 CONVENCIÓN DE ASEGURADORES AMIS

PRINCIPIA UNDERWRITING

Breach incidents

Mossack Fonseca 'Panama Papers'

- Breach of an email server last year

- Described as the biggest document leak ever 11.5 million documents and 2.6 TB of data

- The leak has exposed the offshore activities of hundreds of politicians and public figures around the world, naming Iceland's prime minister David Gunnlaugsson, the late father of British PM David Cameron, Vladimir Putin, and many others

Breach incidents

Ashley Madison:

- Online dating service and social networking service marketed to people who are married or in a committed relationship
- July 2015 group calling itself "The Impact Team" stole the user data of 37m users
- Profile information, including the names, street addresses, and dates of birth of users.

Breach incidents

Ashley Madison

- Users whose details were leaked filed a $567 million class-action lawsuit against Avid Dating Life and Avid Media, the owners of Ashley Madison

- CEO has subsequently resigned

Breach incidents

Anthem

- Anthem Inc. is a US health insurance company founded in the 1940s
- It is the largest for-profit managed health care company in the Blue Cross and Blue Shield Association
- On February 4, 2015, Anthem, Inc. disclosed that criminal hackers had broken into its servers and potentially stolen over 78.8 million records that contain personally identifiable information from its servers

Breach incidents

Anthem

- The compromised information contained names, birthdates, medical IDs, social security numbers, street addresses, e-mail addresses and employment information, including income data.

Breach incidents

Anthem

- Under HIPAA (Health Insurance Portability and Accountability Act of 1996) PHI does not have to be encrypted.
- However Anthem could face civil lawsuits for not having this data encrypted.
- It has been reported that Anthem's $100m Cyber tower may be exhausted on notification alone.

Breach incidents

Nantaz

- Natanz is an Iranian hardened Fuel Enrichment Plant (FEP)
- On 23 November 2010 it was announced that uranium enrichment at Natanz had ceased several times because of a series of major technical problems (supposedly the shutdown of some of its centrifuges)

Breach incidents

Nantaz

- Stuxnet malware infiltration, seemed to be designed to force a change in the centrifuge's rotor speed, first raising the speed and then lowering it
- Intended to induce excessive vibrations or distortions that would destroy the centrifuge.

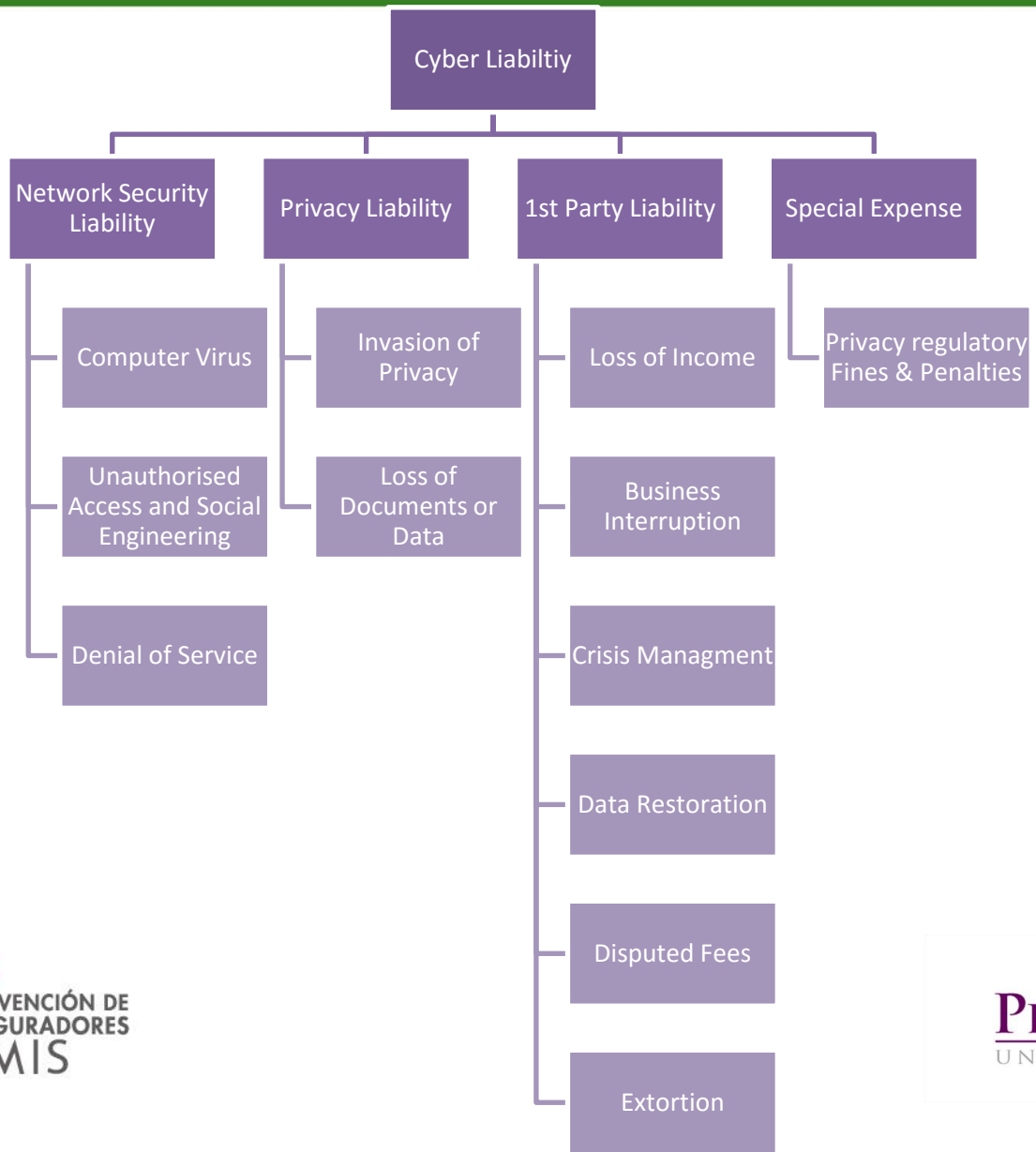
SO....

Cyber Insurance

- Massive increase in interest in cover to respond to the consequences of breach and denial of service attacks

- Cyber is a catch all term

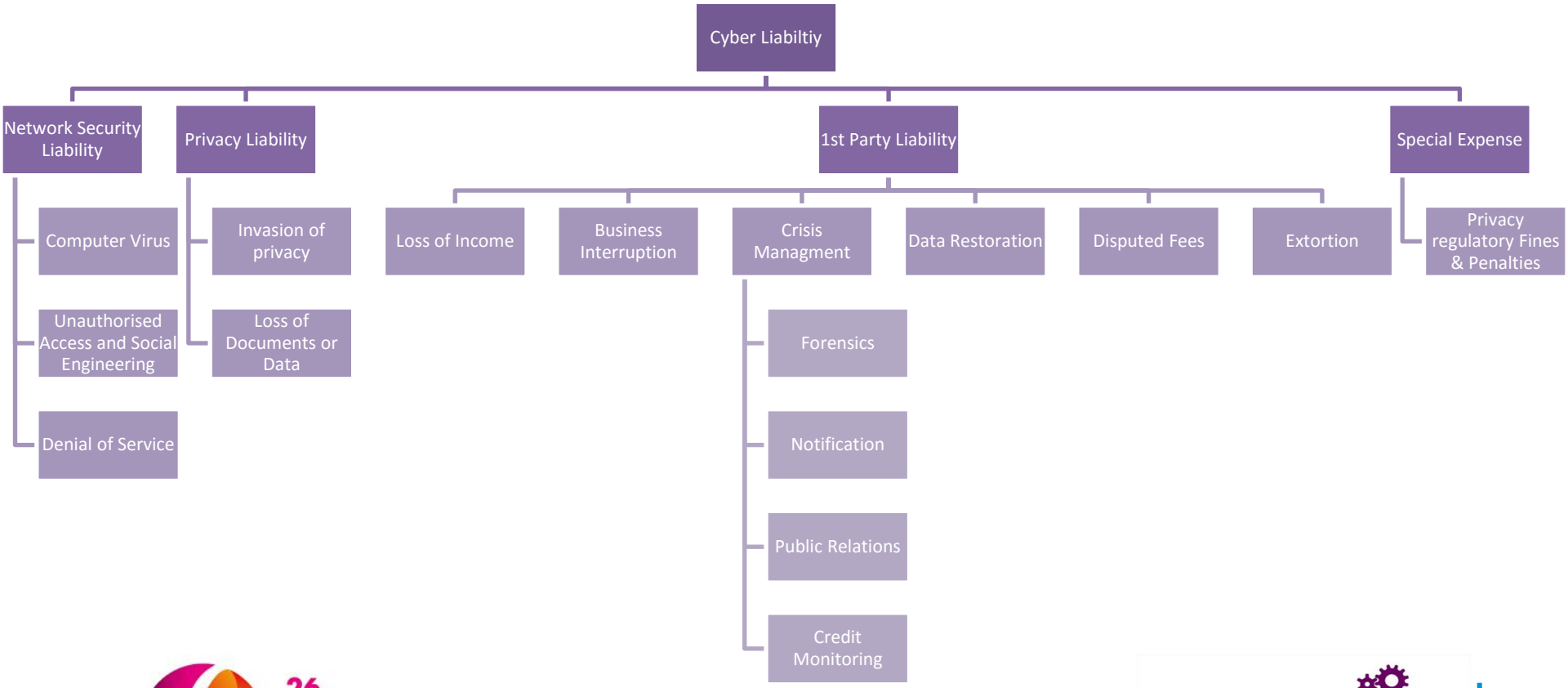
Cyber Liability



26 CONVENCIÓN DE ASEGURADORES AMIS

PRINCIPIA UNDERWRITING

Cyber Liability



26 CONVENCIÓN DE ASEGURADORES AMIS

PRINCIPIA UNDERWRITING

Cyber Insurance

- Only one part of the cyber risk management cycle
- Will continue to develop in terms of sophistication and service
- Alligned with technical services pre- and post-breach
- One of the many tools available to buyers to manage their exposure

INNOVACIÓN, TECNOLOGÍA Y SEGUROS

Sesiones Daños - Ponencia 4

Cyber Risks Business Impact

PRINCIPIA UNDERWRITING

26 CONVENCIÓN DE ASEGURADORES AMIS

Thanks for your attention

Chris Newton, Principia Underwriting

19 de abril 2016