PRIMA'S 2017 RISK MANAGEMENT
WEBINAR SERIES

Cyber & Privacy Liability and Technology E&O

Risks and Coverage

Geoff Kinsella
Partner

Safeonline™



http://map.norsecorp.com

http://www.youtube.com/watch?v=F7pYHN9iC9I

Presentation Overview

1. The Cyber Evolution
2. The Growing Risk
3. What are the cyber risks and costs?
4. My Insurance Market Perspective
5. Risk Management considerations
6. The role of insurance in mitigating cyber risk
7. What does Technology E&O cover?
8. Who needs Technology E&O Insurance?
9. Q&A



The Cyber Evolution

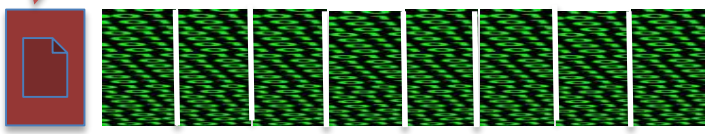
- Dates back to the 1990s;
- Evolution driven by:
  - Internet explosion
  - Dotcom Boom
  - Millennium Bug
  - Civil Law and Regulations
  - Industry specific drivers
  - Third Party Services



The growing risk…

10%of the data currently exists was created pre-2014

90% of this data was created in the last two years

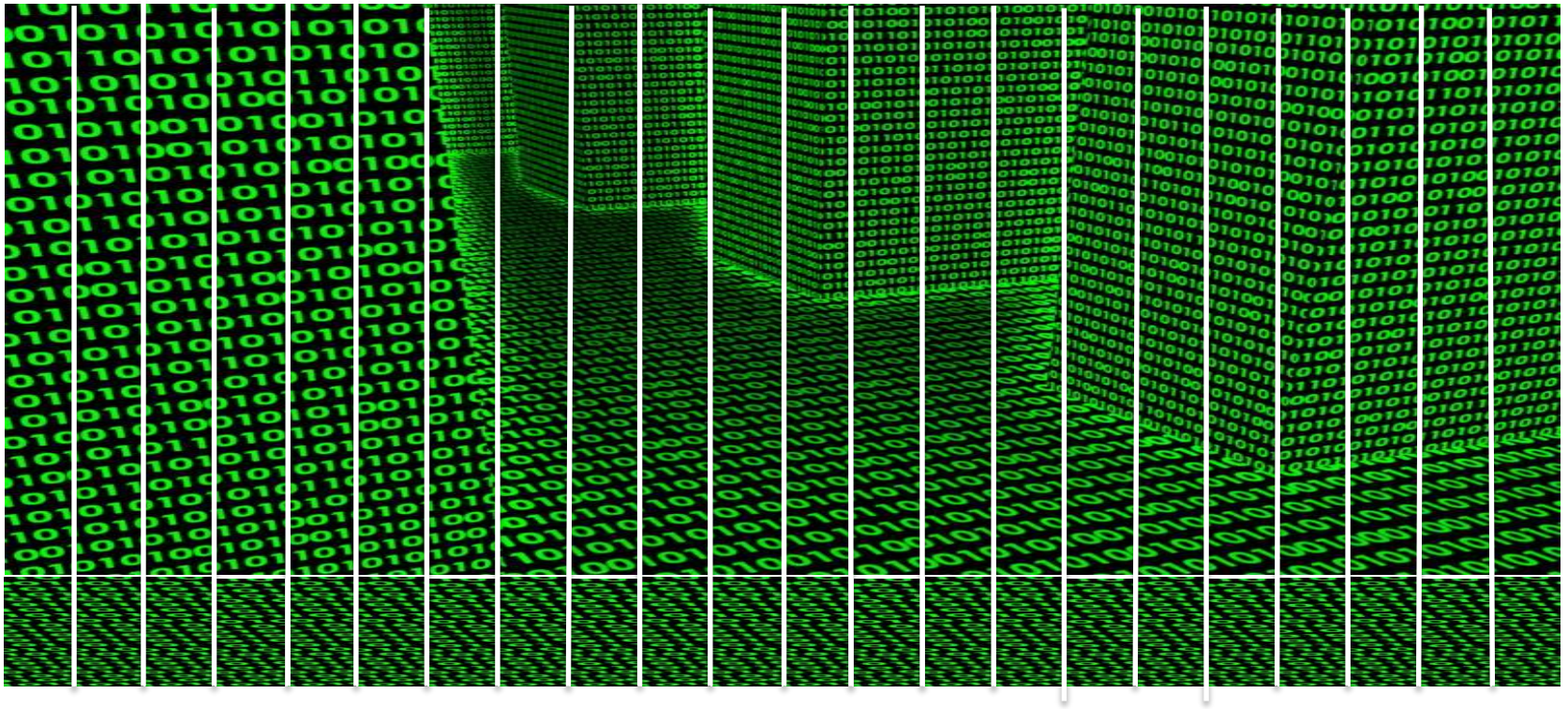




Where will be by 2020 ?

By 2020..

…the volume of data we have will increase by 50 times



Increasing importance of data and systems



Source: internetlivestats.com

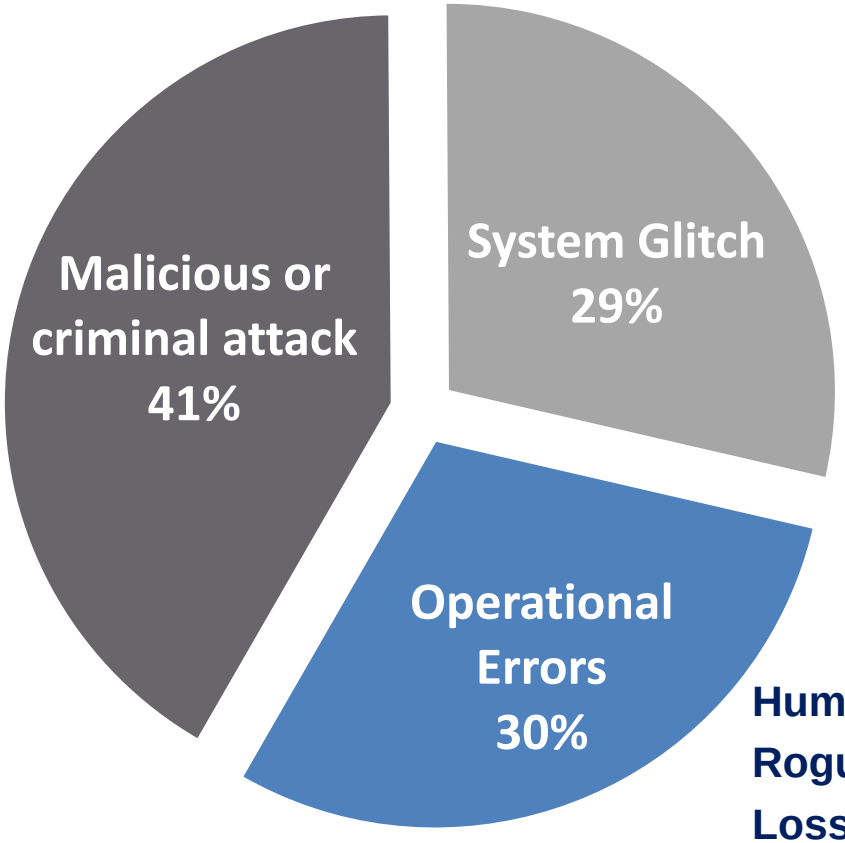
The cause for concern

- Increasing moral and legal obligation to protect our customers' rights to privacy
  - GDPR
- IT Security & regulation not moving as quickly as cyber criminals
- The rapid digitisation of consumers' lives and enterprise records will increase the cost of data breaches to $2.1 trillion globally by 2019
- Systemic Exposures and Aggregation
- The uncertainty of how Cyber Risks affect other insurance classes
- Interestingly criminal activity only accounts for around 41% of cyber losses

What are cyber Risks?

Insurance Triggers for cyber losses

Hacking
DDoS attacks
Malware
Extortion
Social engineering
Cyber Terrorism

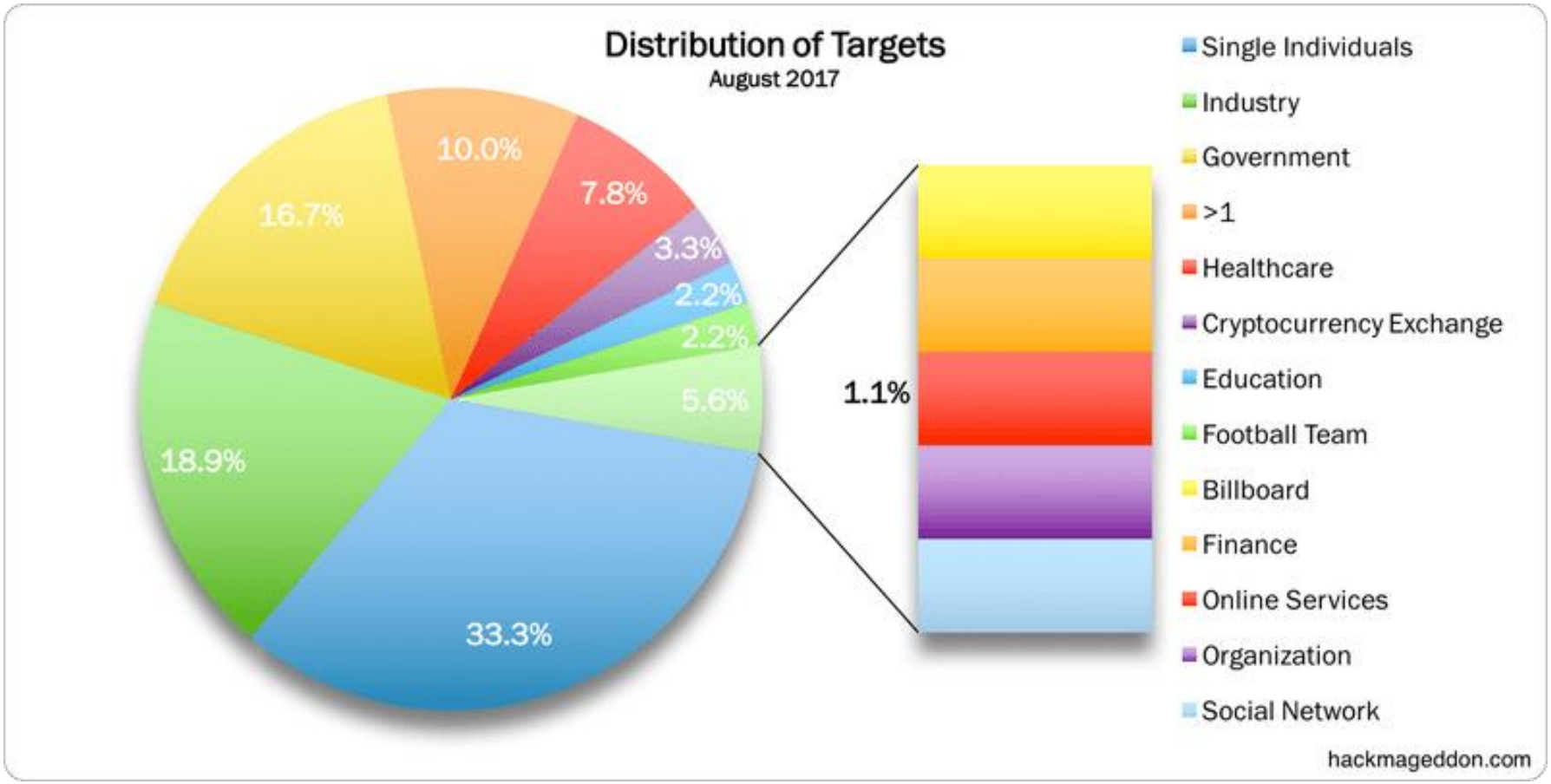


Software bug
Error in coding

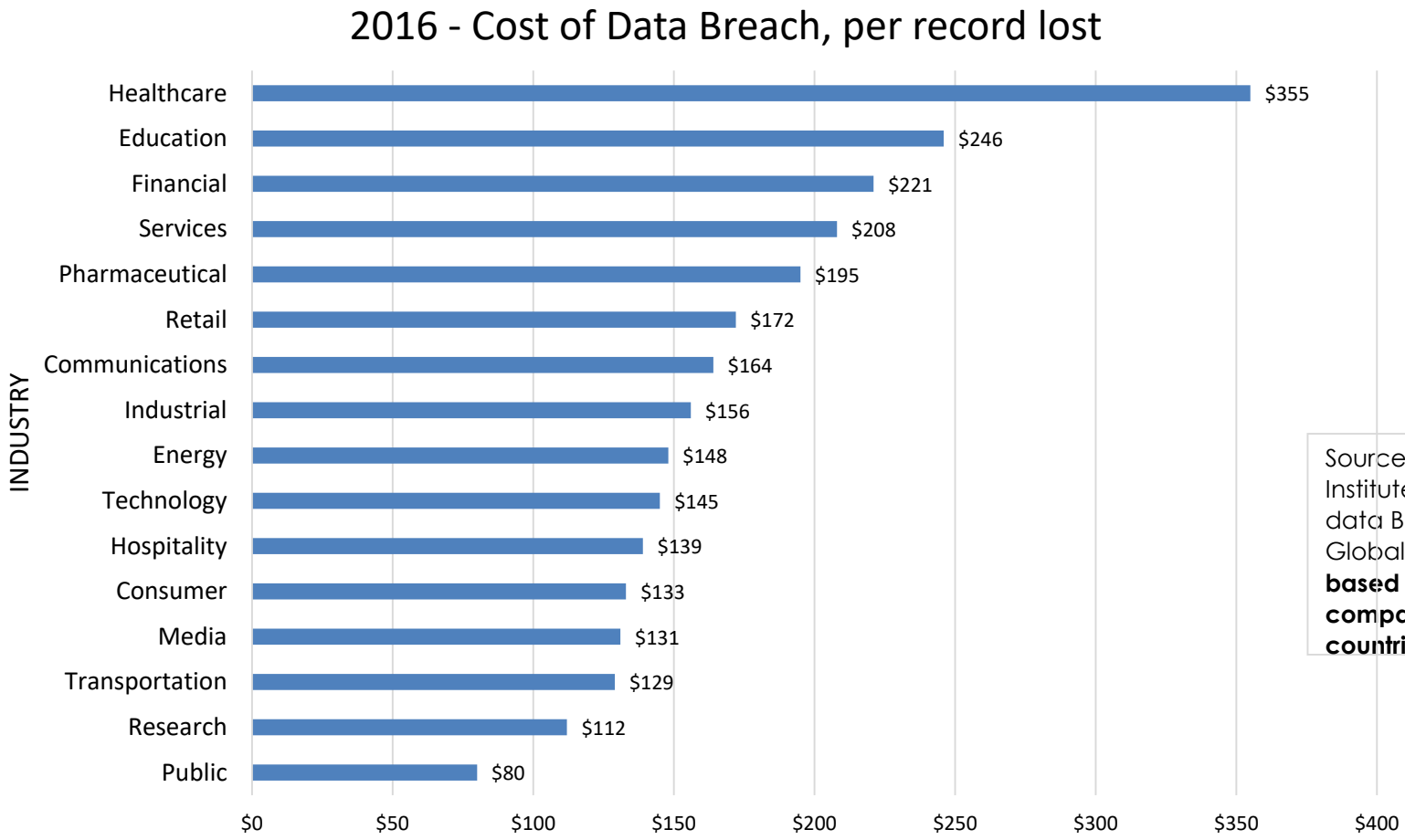
Human error
Rogue employees
Loss or theft of devices
Loss or theft of documents

Source: Symnantec (2016)

Distribution of Targets chart is led by Single Individuals with 33.3%. Governments grow to 10%



What are the costs?



Source: Ponemon Institute, 2016 (Cost of data Breach Study: Global Analysis). **Data based on results from 350 companies across 11 countries**

What are Cyber Risks?

First Party

- Loss or damage to digital assets
- Non-physical business interruption and extra expense
- Cyber extortion and cyber terrorism
- Reputational harm

computer crime and computer attacks by third parties
accidental damage or destruction of hardware
***administrative or operational mistakes* by employees and third party providers**
Full system Failure

Safeonline™

What are Cyber Risks?

Third Party

- Security and Privacy Liability and Defence Costs
  - Network security breaches
  - Transmission of malicious code
  - Damage, alter, corrupt, distort, copy, delete, steal, misuse, or destroy Third Party Digital Assets
  - Breach of third party or employee privacy rights or wrongful disposal of data
  - Causing DDoS attack on third party
  - Phishing or Pharming
  - Confidentiality
- Privacy regulation defence, fines and penalties
- Customer care & reputational expenses
  - Notification expenses
  - Credit monitoring
  - PR expenses
  - Forensics
- Multi-media Liability

Safeonline™

Cyber Insurance Coverage

- **Crisis and Event Management**
  - Security and system failures
  - Network, system and data restoration
  - Notification and call centre costs
  - Fraud and extortion consultation
  - IT forensics
  - PR and reputation mitigation expenses
  - Credit and Identity theft monitoring costs
- **Financial Loss**
  - Business interruption and increased cost of working
  - Cyber theft and extortion
  - Fines and penalties, including PCI-DSS
- **Liability**
  - Privacy liability
  - Security liability
  - Intellectual property and content
- **Legal Expenses**

Safeonline™

Key Underwriting Considerations

- Revenues
- Hazard classes & business activities
- Network security
- Disaster recovery, business continuity & crisis management
- Percentage of on-line revenues
- Dependence on systems
- Internal processes, procedures & employee awareness
- Types & volumes of information stored & how
- Use of mobile devices
- Use of websites, extranets and third-party access
- **Vendors**

Underwriters do not only focus on IT Security

Hack that changed market perception of the risk

- Not the usual method of hacking
- Hacker gained access to a HVAC vendor
- HVAC vendor had file detailing remote log-in details to its clients
- Hacker logged into Target's system
- The hacker was able find both personal data and payment card data

Organisations need to consider vendor access to systems

&

how data is structured internally

Public Sector Issues

- Organic / independent Departmental growth
- Differing agendas to Risk, IT & People
- Data proliferation versus outsourcing
- Vast array of risk areas from hospitals to vehicle licencing from security to Utilities
- Nationalised versus privatised versus, state or federal
- Political targets
- PEST trends key issue
- IT Investment or lack of….

Drivers to Buy

Regulation

Contract

Board

Peers

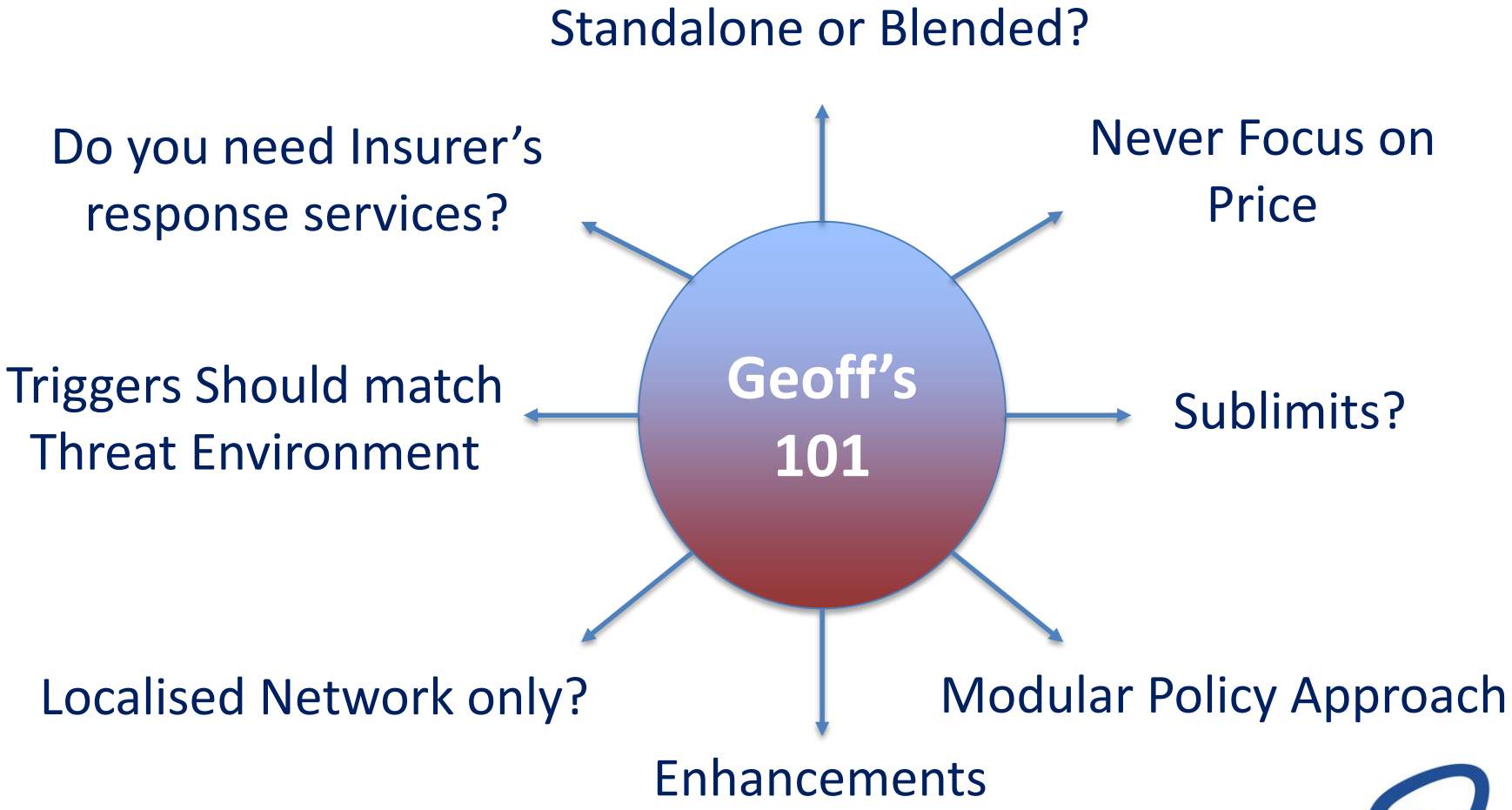
Experience

Pre, During and Post Breach Response



Buying Tips

Insurers will only insure what they want to!



Cover to look out for…..

Enhancements

- Liability extended to cloud providers
- Computer crime, electronic theft & telecommunications fraud
- Programming and human error
- Cyber Terrorism
- Notification Costs outside policy limit – voluntary or legal
- No unencrypted device exclusion
- Forensic Costs to full policy limit
- Social Engineering fraud
  Coverage for volunteers and 'leased employees'
- Punitive Damages - venue
- System Failure –
  - unplanned outages
  - operational errors
- Contingent Business Interruption

What's next?

- SCADA & Property damage – CL380
- Cyber Wallets/ Cryptocurrencies
- Reputational Harm
- Crisis Management Coverages
- Crime
- Contingent Business Interruption

Industries Most Affected

- Hospitality
  - accommodation
  - food services
- Retail and e-tail
- Financial services
- Healthcare and social services
- Educational institutions
- IT/Technology entities
- Government entities
- Charities

Anyone relying on a network
Anyone relying on a system
Anyone storing or processing data
Anyone with a presence online

My Insurance Market Perspective



http://www.youtube.com/watch?v=F7pYHN9iC9I

THE WILD WEST!



WHY?

- Area of growth in depressed market;
- Proliferation of new entrants;
- High Profile Media Focus;
- Premium Volume Expectations:
  - $2.5BN up from $1BN in 2012;
  - $8BN by 2020.
- Young inexperienced participants

Is this good for you the BUYER?

Cyber Gold Rush!

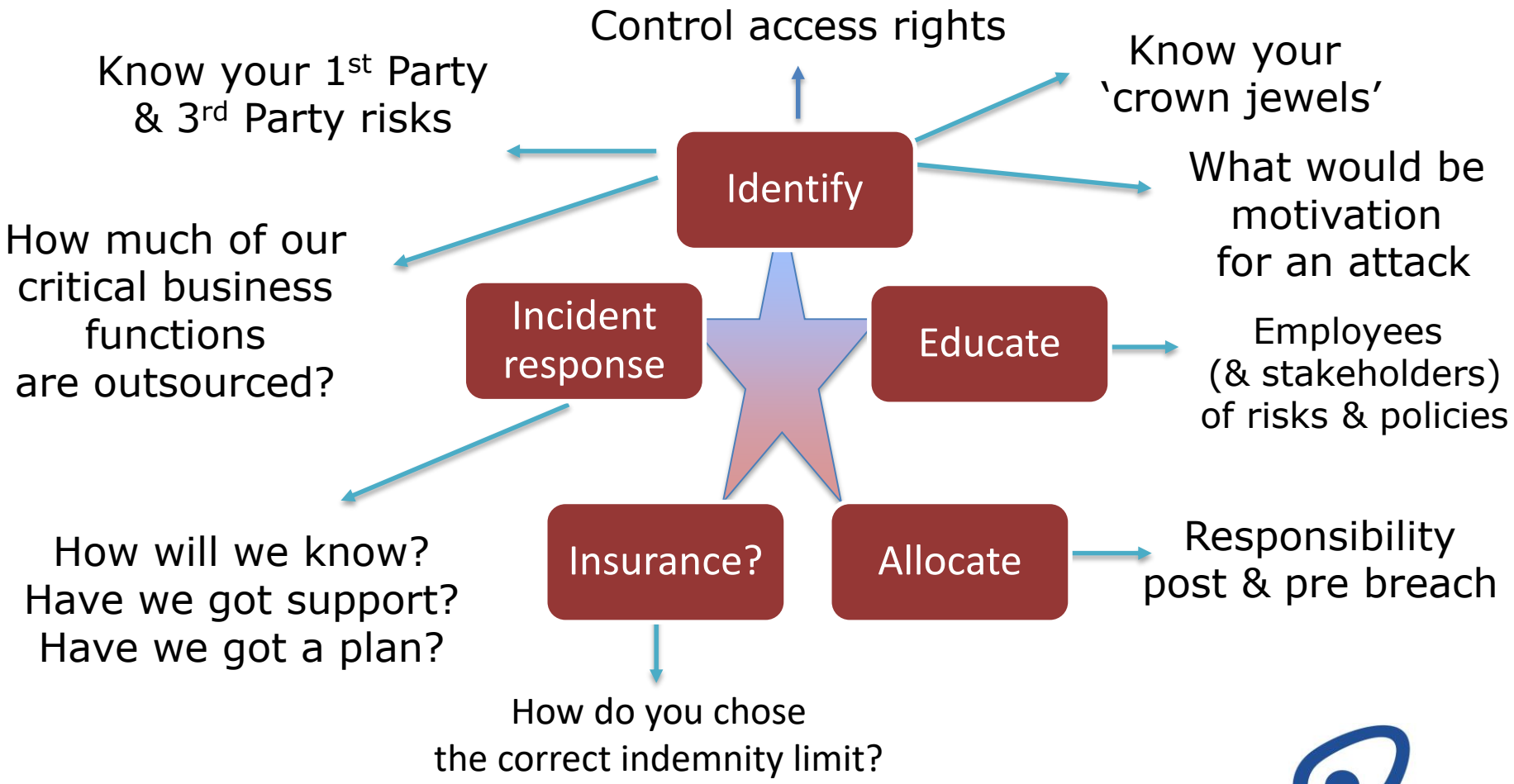


Risk Management Considerations

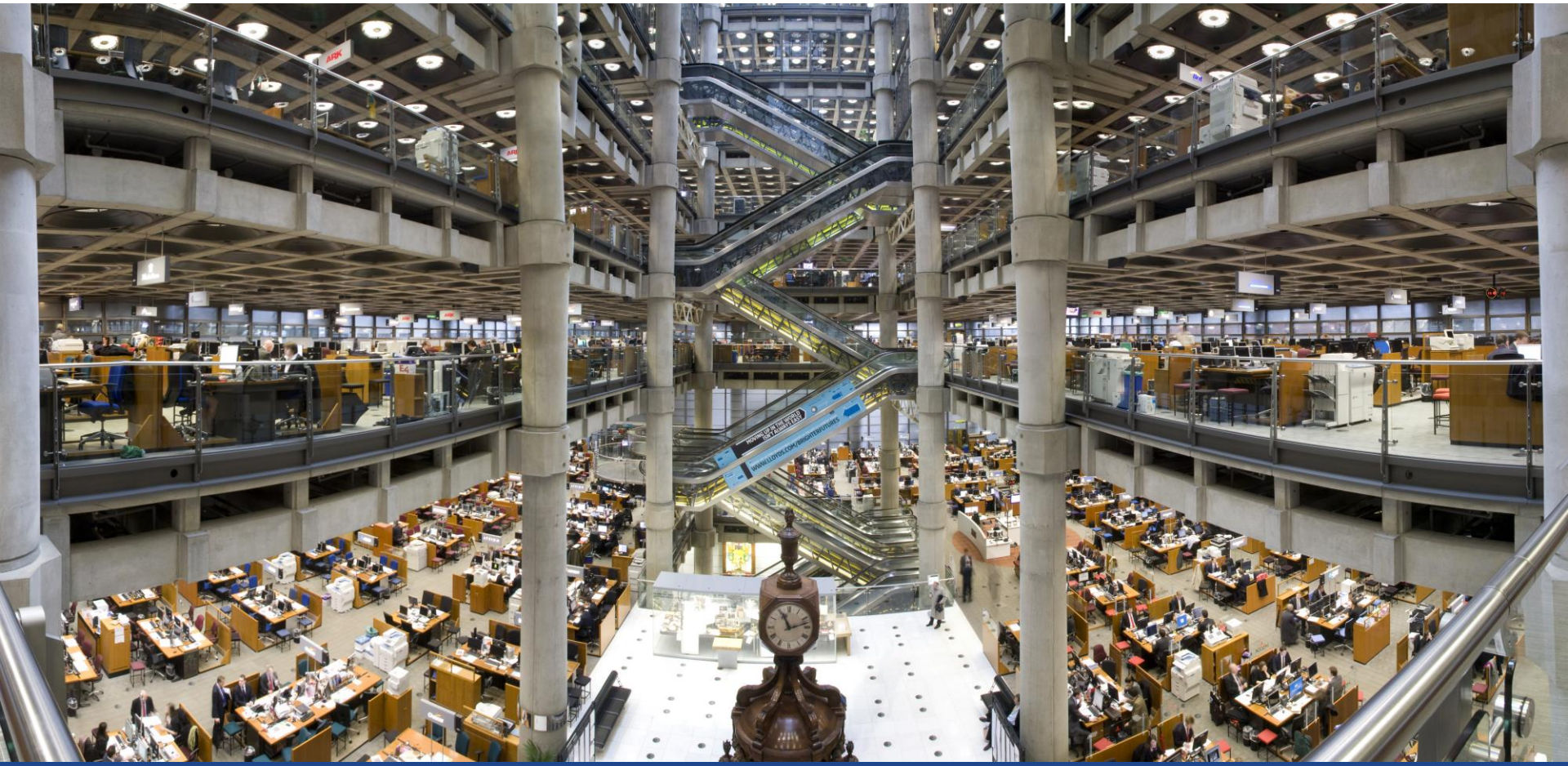


Risk Management Considerations

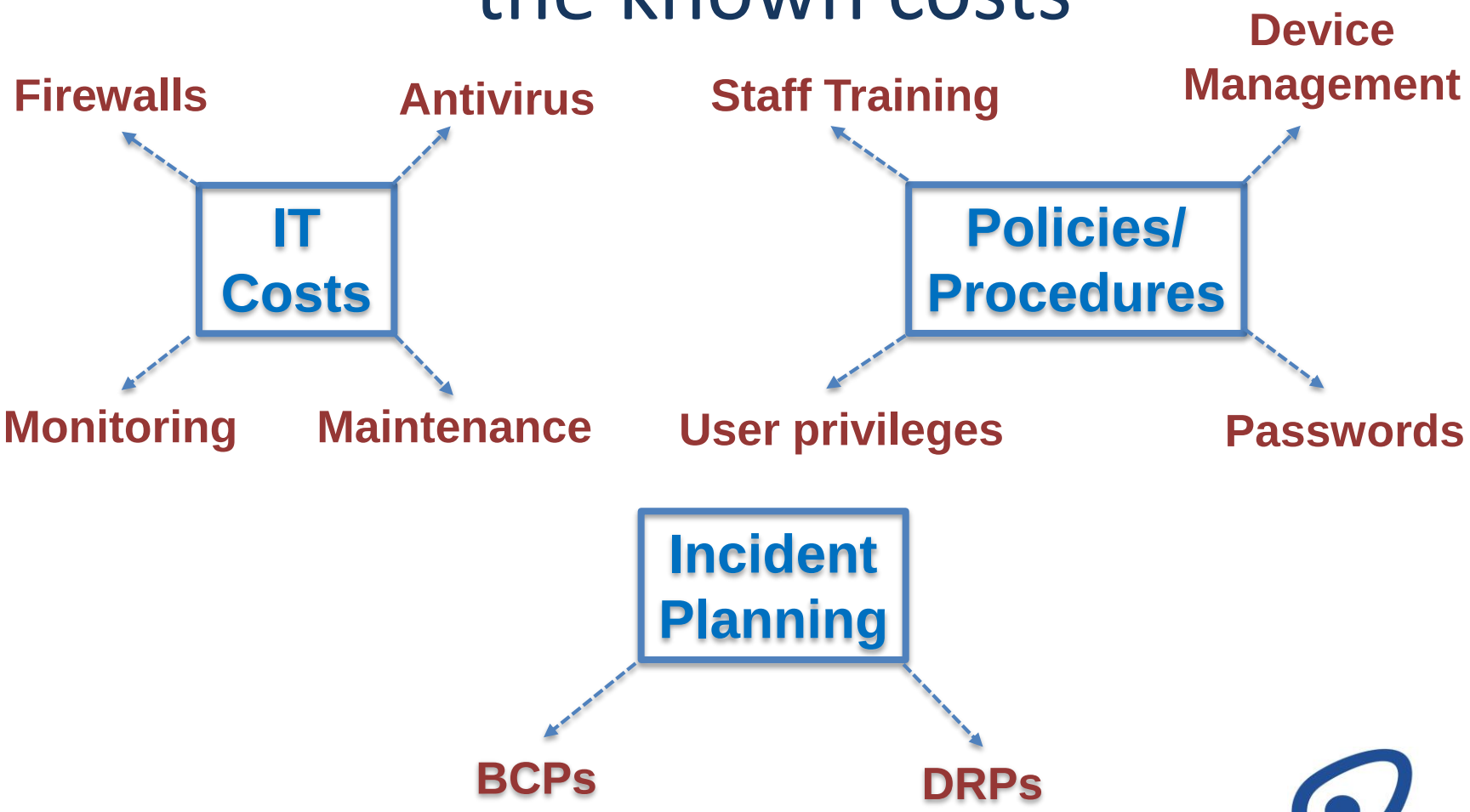
Must be part of your overall ERM programme



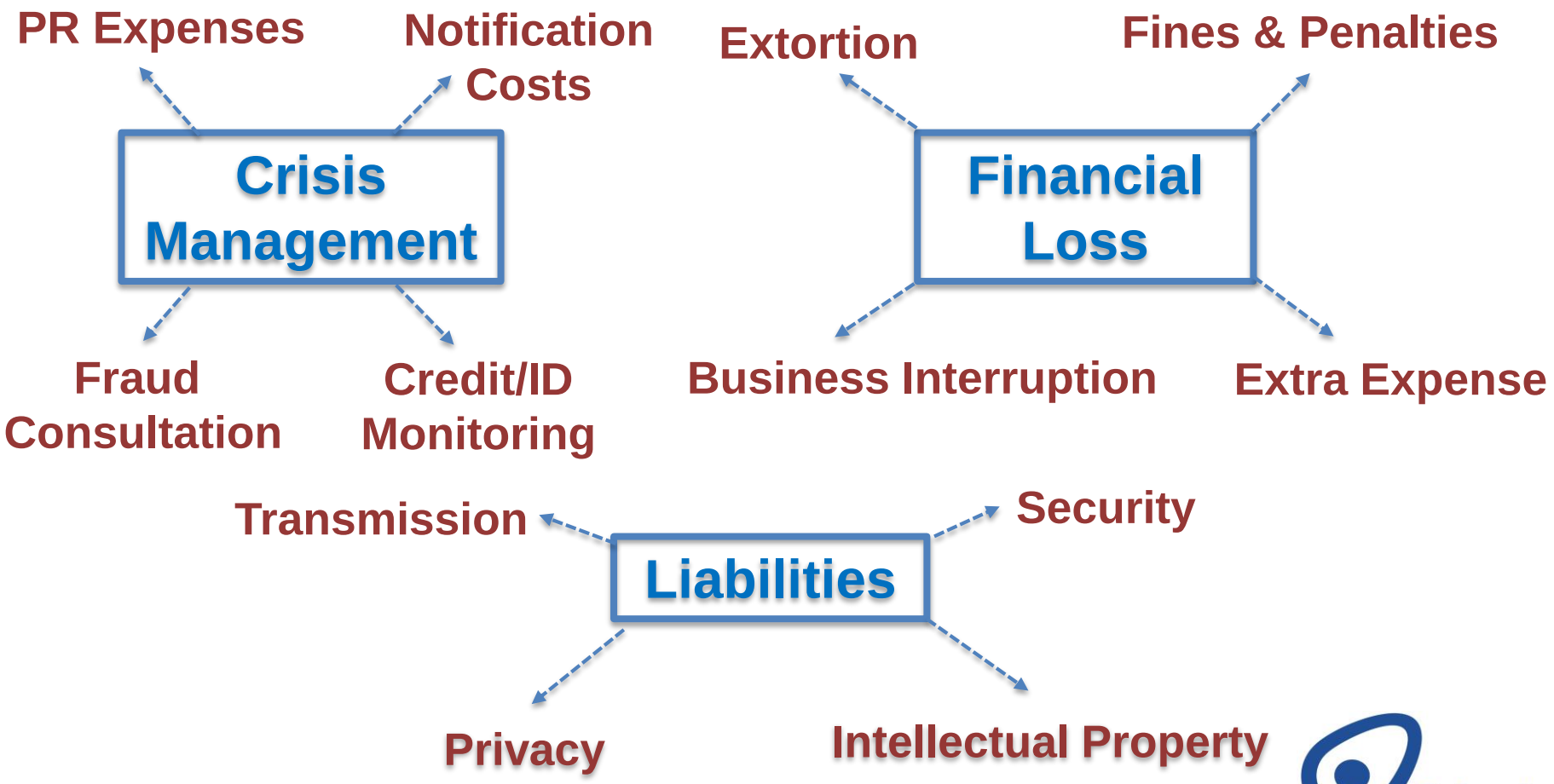
The role of insurance in mitigating cyber risk



Cyber Risk Management
the known costs



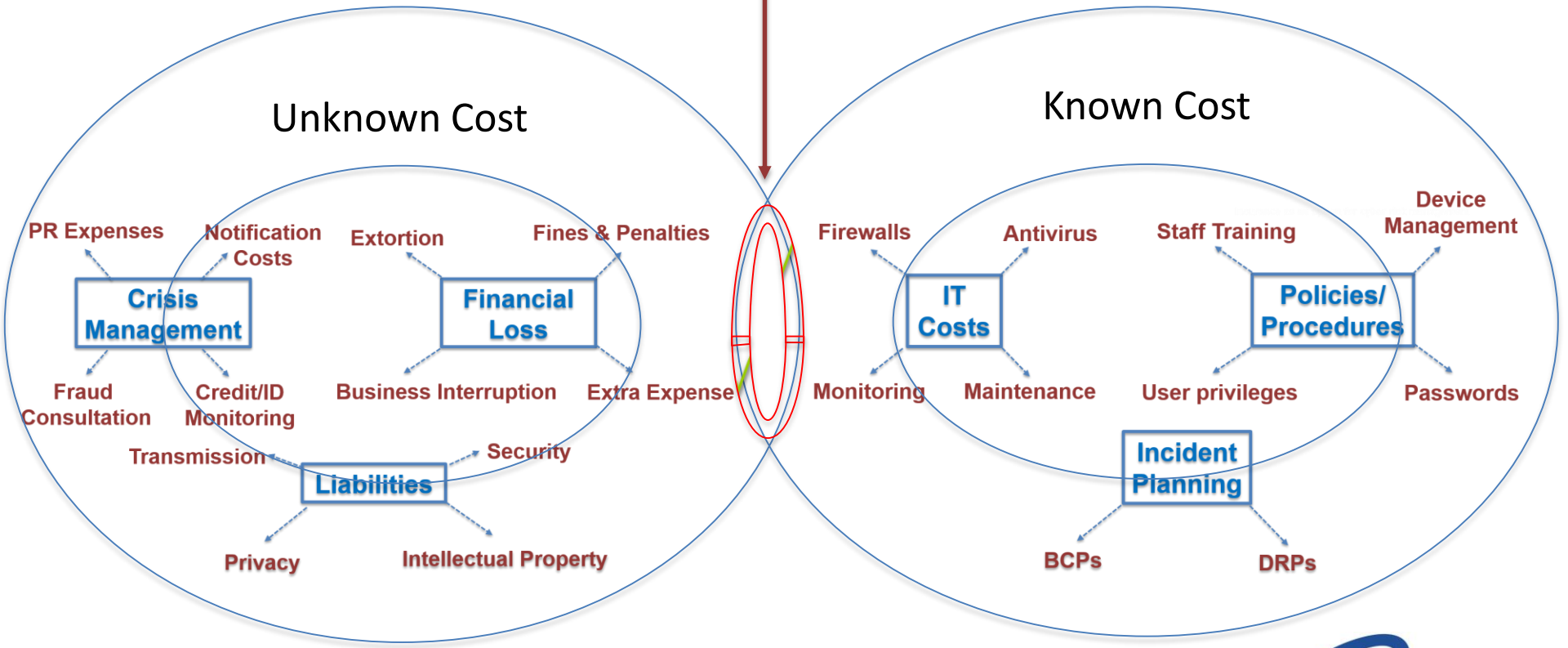
Cyber Risk Management
the Unknown costs



Safeonline™

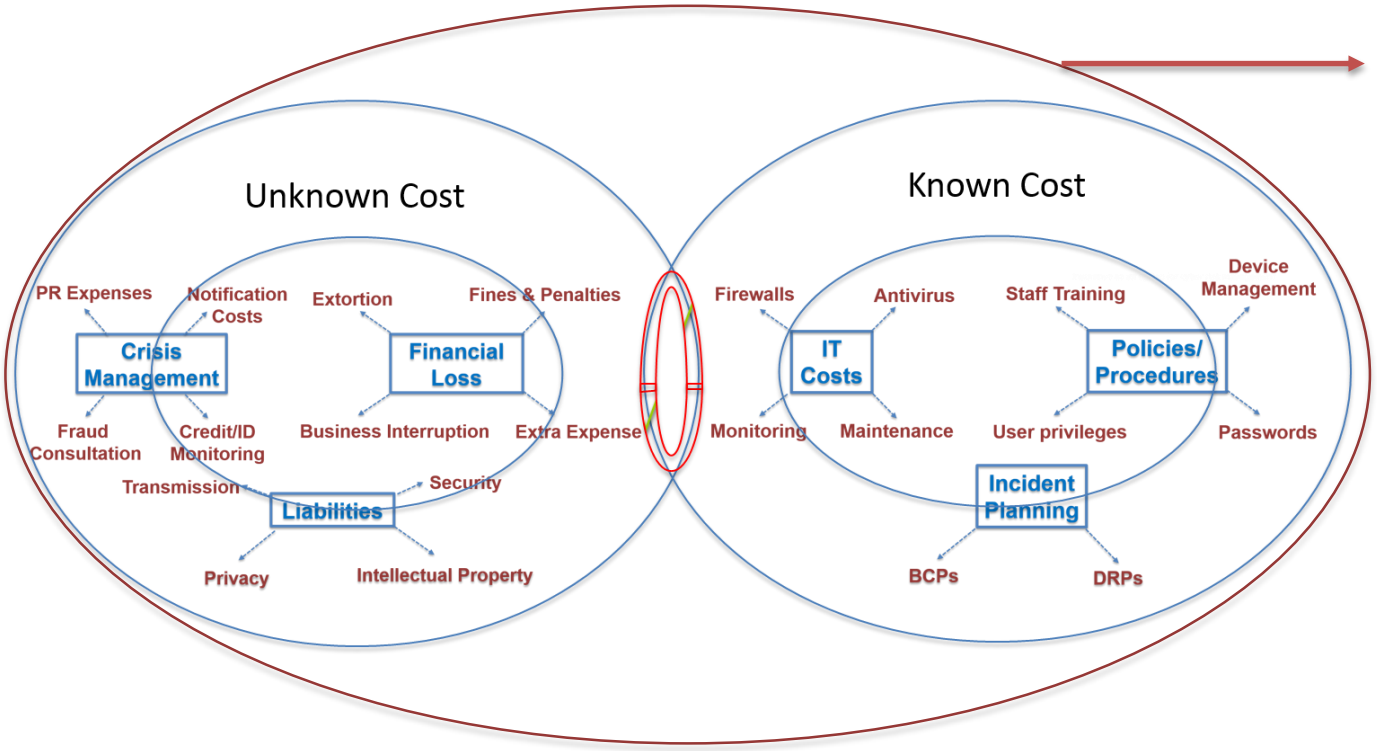
Cyber Risk Management

So how and where does a cyber insurance policy fit in?



Safeonline™

Cyber Insurance



Cyber Insurance

- Enables budgeting certainty of cyber risk management programme
- Financial protection from unknown costs
- Rapid response from specialist crisis response teams
- Pre-, during-, and post-breach services
- The cyber insurance policy will only cost a fraction of the overall spend on cyber risk management



Technology E&O Insurance



http://www.youtube.com/watch?v=F7pYHN9iC9I

What is Tech E&0 insurance?

Tech E&O insurance is intended to cover two basic risks:

(1) financial loss of a third party arising from failure of the insured's product to perform as intended or expected, and

(2) financial loss of a third party arising from an act, error, or omission committed in the course of the insured's performance of services for another.

Legal Liability policy:

Pay sums you are legally obliged to pay (including costs & expenses) for:

Negligent act, error, omissions,

Misrepresentation

Breach of contract

Senior employee dishonesty

Act or error etc. giving rise to a Civil liability.

Arising out of your business activities performed for a client

Cover to look out for…..

Enhancements

- Breach of Contract
- Loss of Documents
- Fidelity of Employees
- Intellectual Property Rights
- Products Liability
  - Property
  - Bodily Injury
- Defamation (media liability)
- Waiver of Subrogation Rights
- Refund of Fees



Who should buy Tech E&0?

Traditionally designed for providers of technology services or products

Companies such as data storage, web designers, software developers and hardware manufacturers, IT services companies, help desk services, domain name resellers, telecommunication resellers, network engineers etc.

Lines now becoming more blurred as traditional offline companies enter the technology development/ service field

Do any of your entities provide technology services?

Exxon, Amex, GE, Citi, Target, JP Morgan, and Walmart are all racing to become technology companies. Telsa is a technology company racing to become a car company!

Key Underwriting Considerations

Revenues by activities e.g.

- Hardware
  - Own manufacturing
  - Resale hardware
  - Installation
  - Maintenance
  - Dependence on systems
- Software
  - Coding or no coding
  - Maintenance
  - System Integration
- Services
  - Consultancy /Contracting
  - Training
  - Hosting or processing

Other considerations:

- Nature of Activities
- Client profile/ examples
- Number of Customers
- Contract examples
- What are consequences of failure?
- Losses

‘Blending Cyber and Technology E&O helps to alleviate the potential of losses falling between the cracks’

Insurers are now offering a modular approach

Questions?



Cyber & Privacy Liability and Technology E&0

Risks and Coverage

Geoff Kinsella
Partner

Safeonline™

