

iapf 
representing pension savers



Seminar



What's your cyber defence?

Thursday 27 February 2020



Welcome

Jerry Moriarty
CEO, IAPF

House keeping

NOTE EMERGENCY EXITS
PUT MOBILE DEVICES ON SILENT
FILL IN EVALUATION FORMS
DOWNLOAD PRESENTATIONS AT
WWW.IAPF.IE



What's your cyber defence?

Vanessa Jaeger
Principal Consultant, Aon



NIST Cyber Framework



1. Prevention
2. Identify issues
3. Managing response

Tabletop rules

Be honest

- The tabletop is a learning tool first and foremost, so play honestly
- The exercise works best if you try not to fight it

Ask questions

- Q&A session at the end

You are the chair of trustees

- For this scenario you can assume that you are Alex, the Chair of Trustees

Accept the situation

- The scenario might not be completely realistic for your scheme
- The exercise is more about the actions rather than the how, so embrace this




Inject one

Situation

On Thursday morning Alex receives a call from Susan the HR manager at ABC Limited, informing her that they have received a number of enquiries about a Trustee exercise to verify member details for the pension scheme. The request asks for confirmation of the member's PPS Number, as well as bank statements and utility bills. She's rather concerned that this is the first the sponsor has been made aware of this and also queries whether it is a breach of data protection issues.

It's the first time that Alex has heard of the exercise. She is sure that neither the Trustees or administrators would have done this



What would you do in this situation?



Inject two



Situation

Alex has made a number of calls, including to Michael the client manager at XYZ Administrators and to other Trustees (although she's not managed to get hold of them all)

Michael calls back at 2.30pm. He's reviewed the Scheme's activity logs and can confirm that there has been a significant increase in member requests, including an unusual volume of requests to amend personal details, early retirement quotes and changes to bank details.

He confirms that the letter was certainly not from them.

Is there anything else you would like them to do, such as not processing new requests or changing back the ones they've done recently? He also asks whether to put the DC benefit statements on hold.



How do you respond?



Inject three



Situation

Later that day, Michael calls back. They've been notified of a cyber attack at their printing provider which appears to be the source of the letters. The original leak was 5 months ago but it has only just been identified.

Reports of the breach have also been leaked to the media and he's unsure if the ABC scheme will be named.

As a precaution, a number of the administration services have been taken offline and individual member payments have been halted. Michael does however ask about the running of the pensioner payroll tomorrow, should this still be run?

One of the Trustees calls to say he's had the same letter and has been encouraging members to return the requested information to ensure that their pension gets paid this month.



What actions
do you take?

Managing response



- Contact details
- Communications checklist
- Media plan
- Reporting requirements
- Additional support
- Lessons learned



Safeguarding for the speed of innovation

Karl Curran
Director - Cyber Practice Leader, Aon



Aon's 2020 Cyber Security Risk Report – What's Now and What's Next?

8 Key Risk Areas



Technology

Embracing digital transformation creates new and unanticipated risks



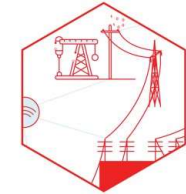
Supply Chain

Supply chain security wake-up calls grow more insistent



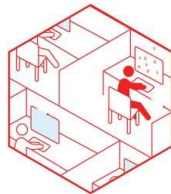
IoT

IoT is everywhere, and it is creating more risks than organisations realise



Business Operations

Technology for operational efficiencies can lead to security deficiencies that disrupt organisations



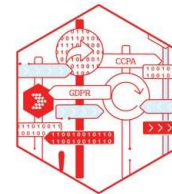
Employees

Excess privileges and shadow IT increase employee risk



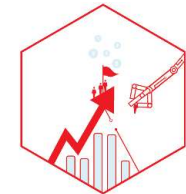
Mergers & Acquisitions

Vulnerabilities from deal targets increases as dramatically as M&A value



Regulatory

Managing the intersection of cyber security policy and enforcement



Board of Directors

Directors and Officers face growing personal liability relative to cyber security oversight

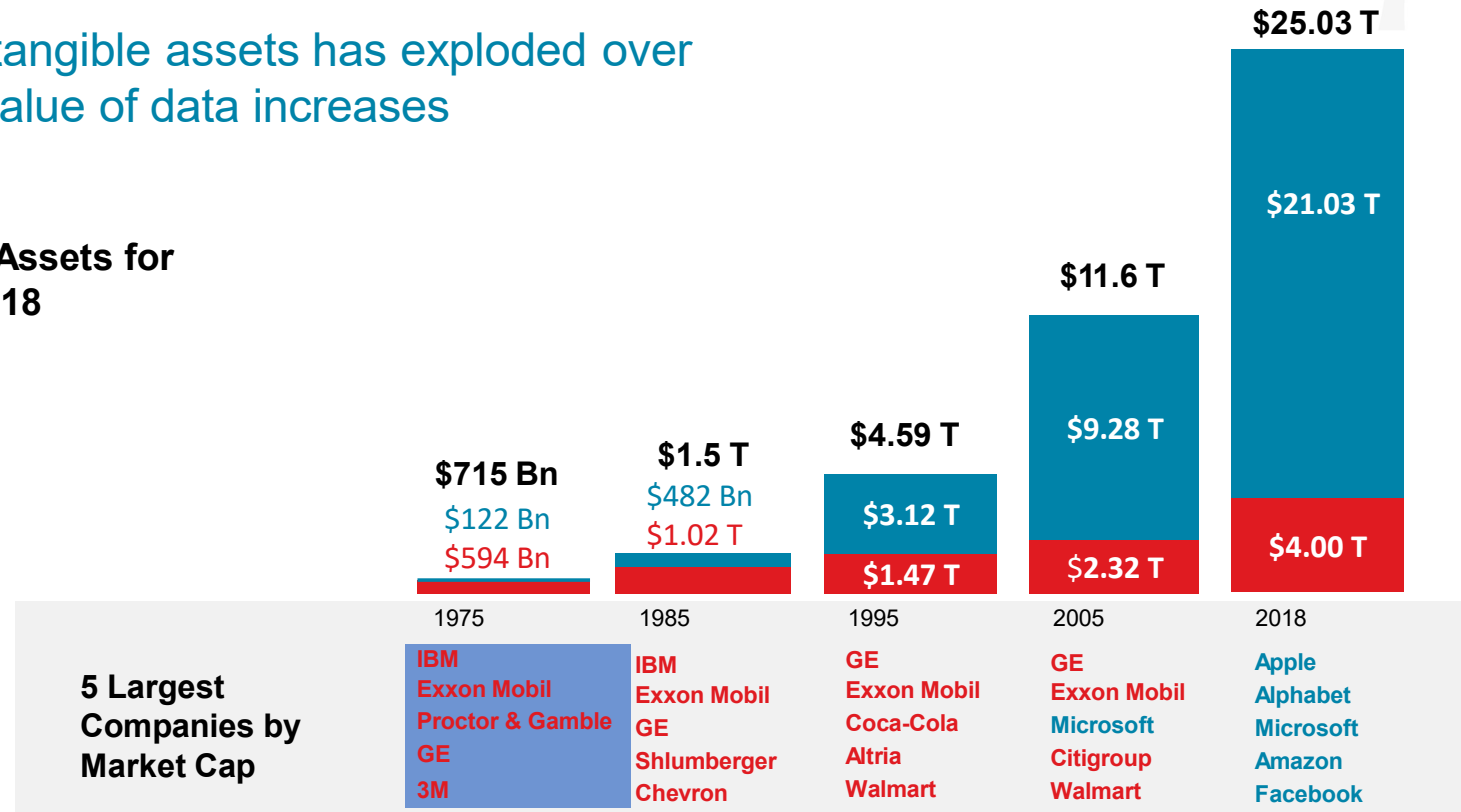
Source:
[Aon's 2019 Cyber Security Risk Report](#)

Historical Evolution from Tangible to Intangible Assets

The ratio of intangible vs tangible assets has exploded over the past 20 years as the value of data increases

Tangible assets vs Intangible Assets for S&P 500 companies, 1975 - 2018

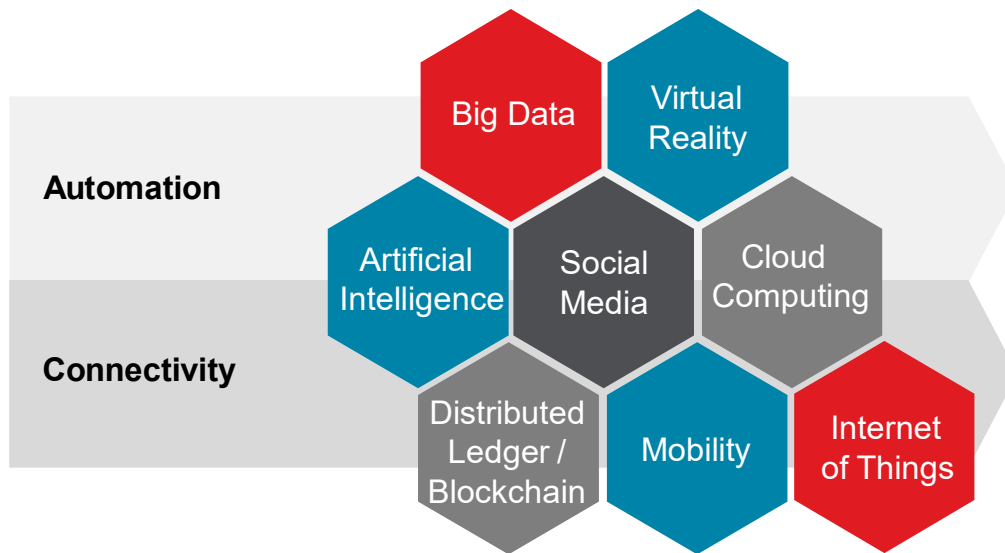
- **Intangible Assets**
 - Difficult to value
 - Difficult to insure
- **Tangible Assets**
 - Easy to value
 - Insurable



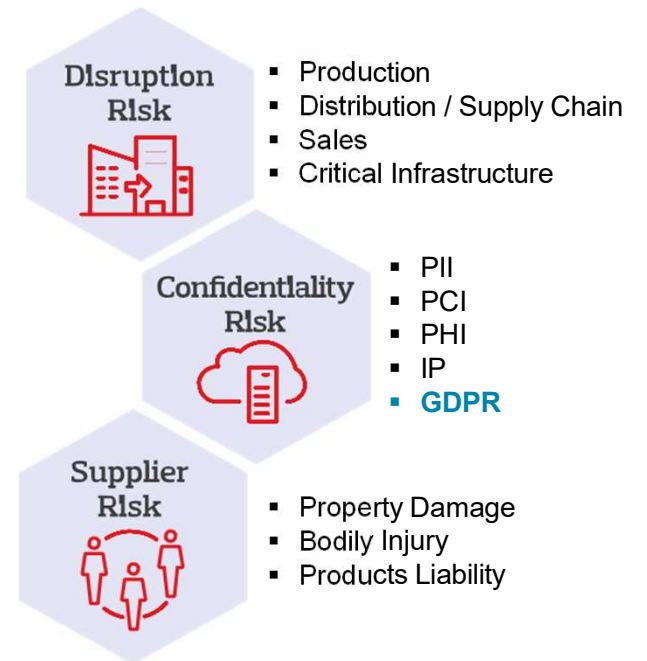
The Evolving Cyber Threat

Organisations across all industries continue to invest in deploying digital technologies to stay competitive and drive quality and efficiency objectives

Economic Drivers



Strategic Threats



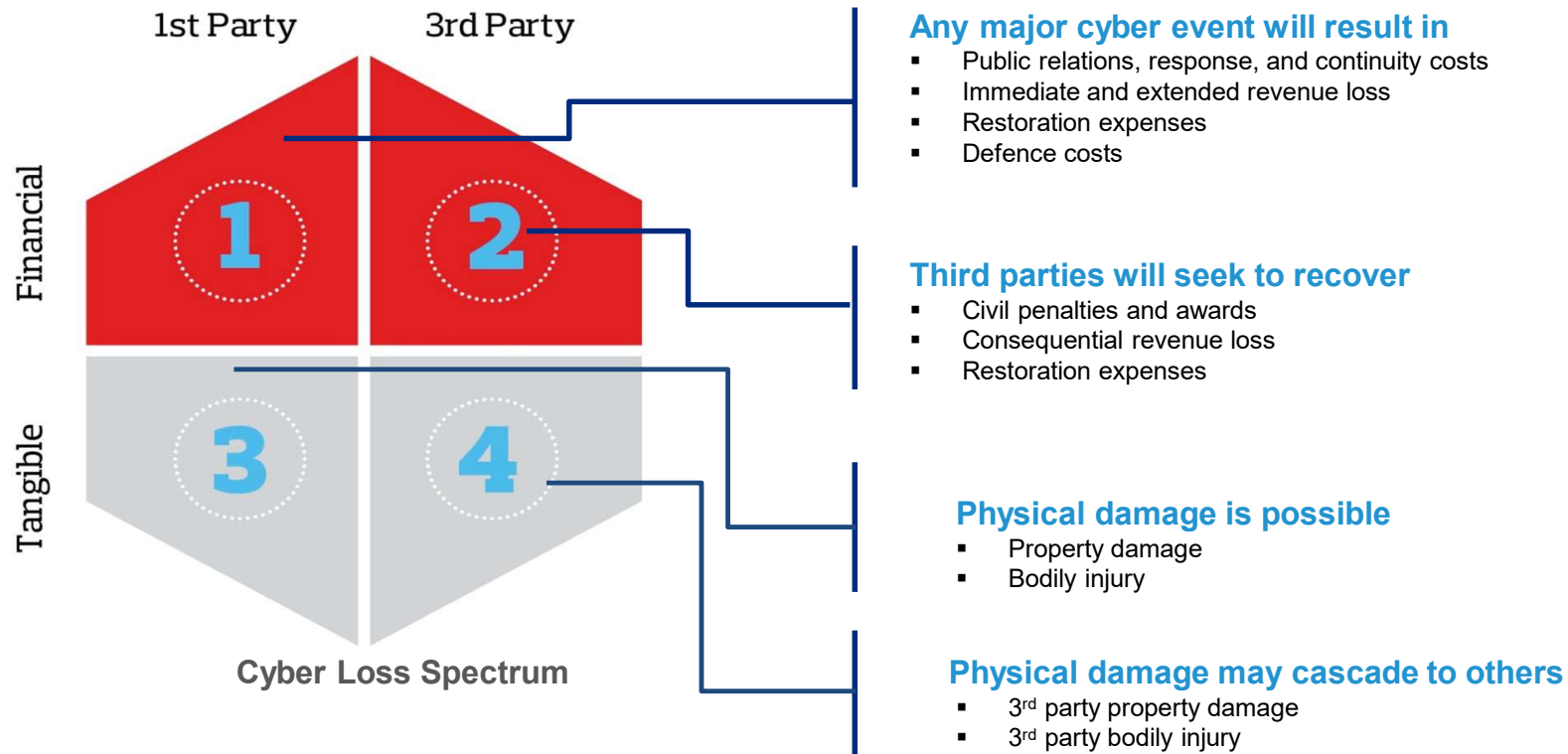
Complexity of the Cyber Challenge

Changes to digital transformation, security threat environment and regulatory landscape.
Risk and Insurance Managers need to take an **enterprise wide approach** to manage cyber risks.



- 
Notification requirement for personal data breaches
- 
Fines up to €20 million or, if higher, 4% of annual global turnover
- 
New duties for data processors + new rights for data subject

Cyber Risk Impacts All Loss Quadrants

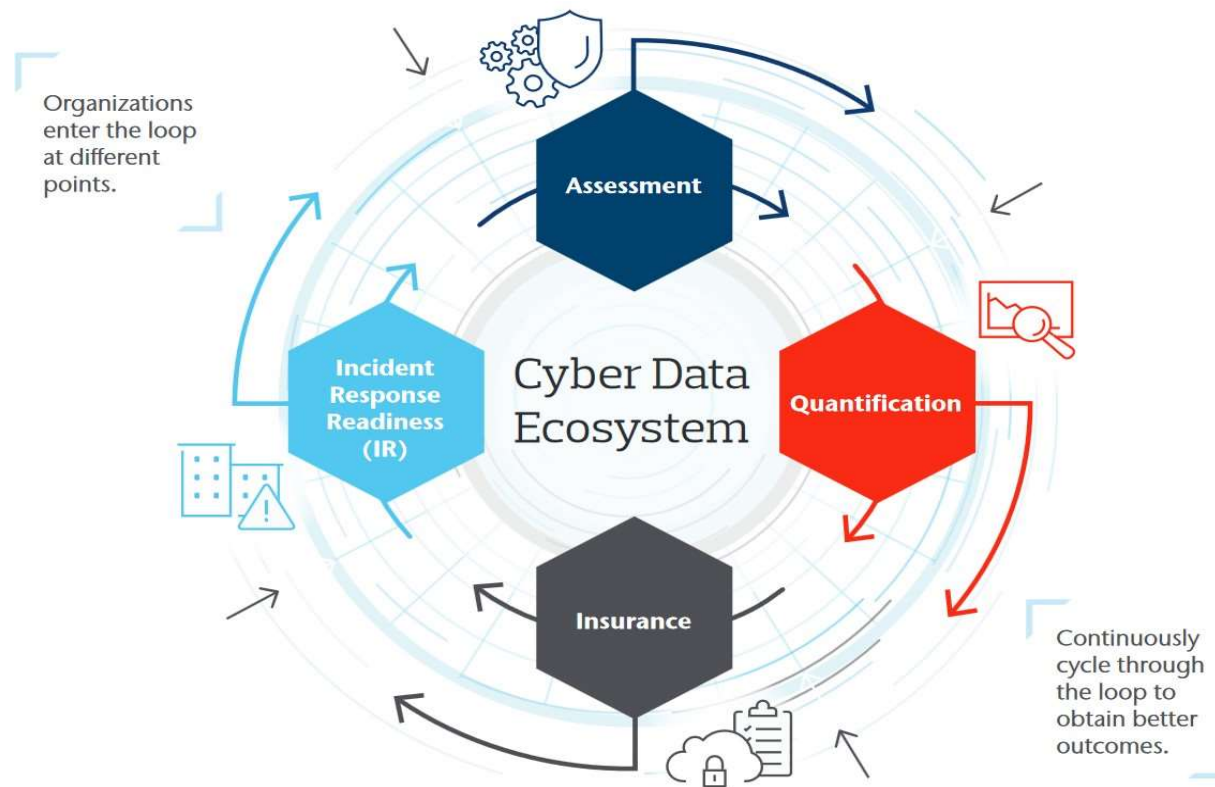


Building Cyber Resilience in an Interconnected World



*Resilience is best achieved by a data-driven, circular strategy, **Aon's Cyber Loop.***

The Cyber Loop: Managing cyber risk requires a circular strategy

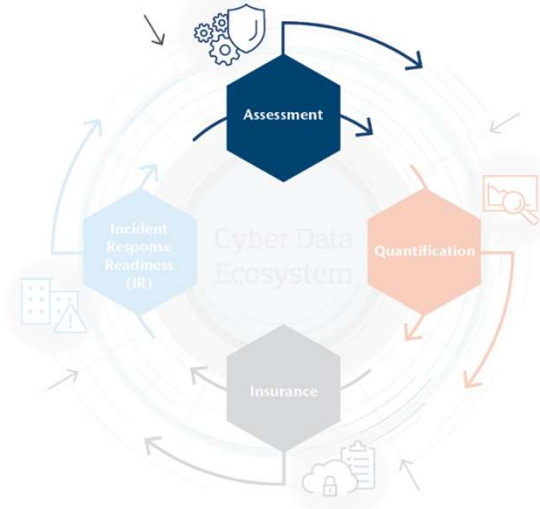


Source: [Aon's White Paper The Cyber Loop](#)

The Cyber Loop Entry Point:

Assessment *Insight is critical to resilience*

Questions answered. Data gathered.



- What are the most important assets we need to protect?
- What are the most likely threats?
- What is the state of our security and controls?
- How do we balance business needs with cyber risks?

1 Avoid the Risk.

Choose to not take the action that introduces the risk.

2 Mitigate the Risk.

Assess and test the risk, and put compensating controls, technologies, processes and governance in place to reduce exposure, while working to minimize impact on the business growth strategy.

3 Accept the Risk.

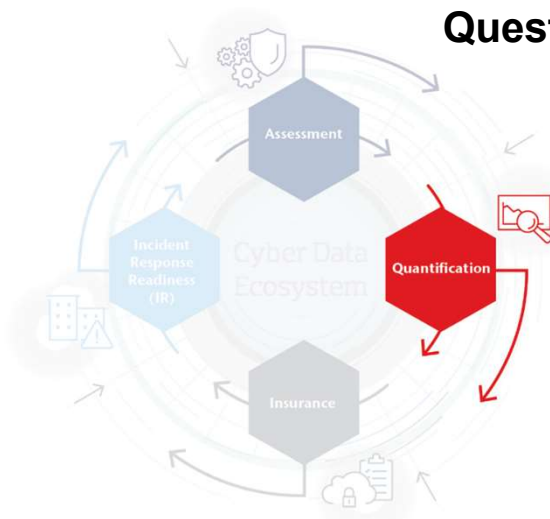
Assess the risk, and choose to accept the risk as is, if mitigation reduces the business benefit the organization set out to achieve.

4 Transfer the Risk.

Seek cyber insurance policies to move the risk off the balance sheet.

The Cyber Loop Entry Point: Quantification *Operational and Balance Sheet Impact*

Questions answered. Data gathered.



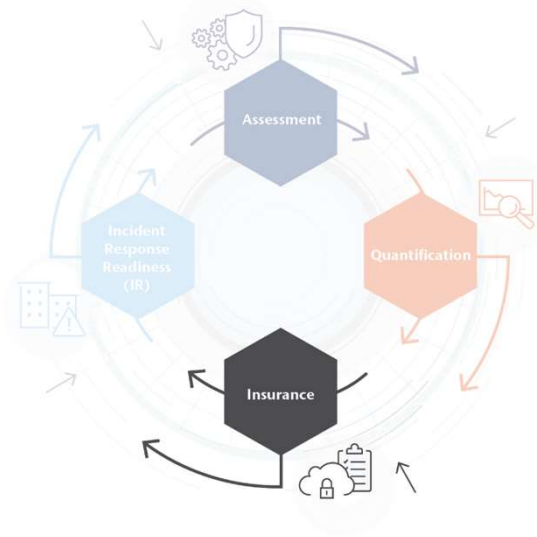
- Do we know the type and materiality of our potential losses?
- How are we making security investment decisions?
- Can we measure the effectiveness of our current risk management and insurance in terms of total cost of risk (TCoR)?



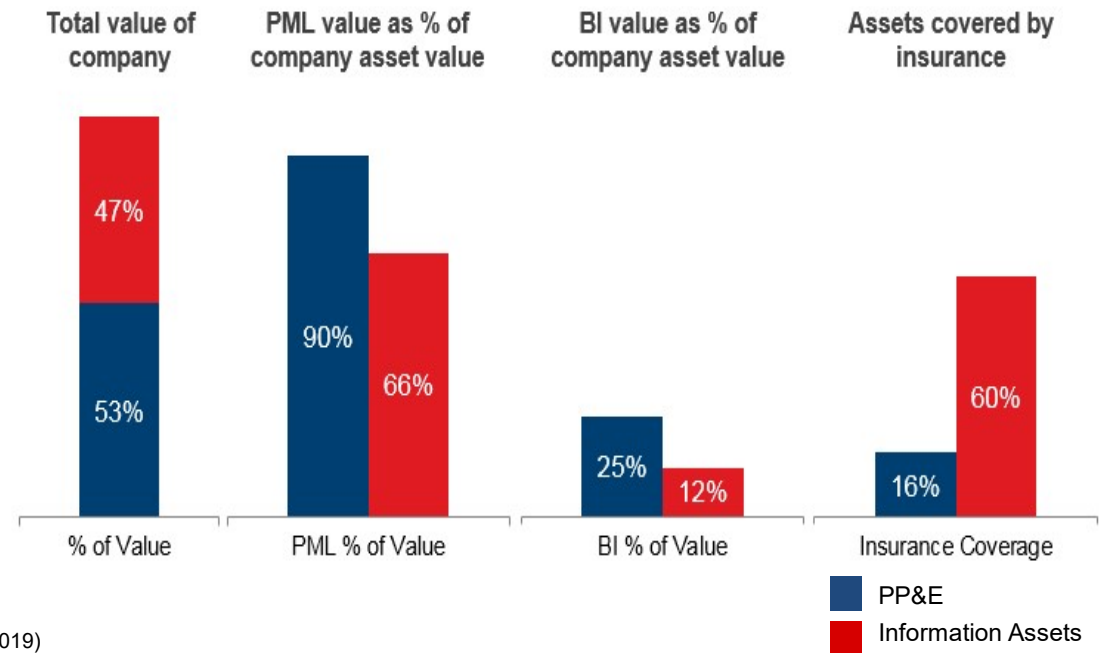
The Cyber Loop Entry Point:

Insurance *Transferring potential financial loss*

Questions answered. Data gathered.



- Do we understand our exposures?
- Do we have an effective strategy to mitigate loss?
- Should we transfer a portion of our risk to the insurance market, or consider alternative risk transfer strategies?

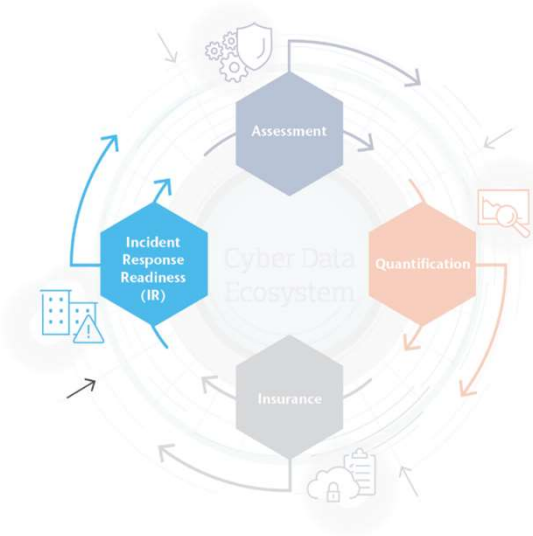


Source: [Aon Ponemon 2019 Intangible Assets Financial Statement Impact Comparison Report](#) (April 2019)

The Cyber Loop Entry Point:

Incident Response Readiness *Incident Preparation and Effective Response*

Questions answered. Data gathered.



- Do we have an appropriate, usable response plan? If yes, is the response team trained and ready to act?
- Is our response team able and ready to respond? Do we have the right security and forensic tools, processes, and procedures? Have we properly configured our cyber security technology?
- Can we quickly and effectively respond to an incident?



Every minute
of an undiscovered,
unaddressed or
uncontained
breach costs
your company
in terms of
reputation
and **monetary**
damages.

Aon's Cyber Risk, Security and Insurance Expertise

Enterprise Wide approach

through cyber assessment, quantification, mitigation, transfer, testing or response solutions

+600

dedicated cyber professionals globally

+5,000

cyber clients

+1,500

company cyber threat and exposure database

12 of 20

largest cyber breaches were managed by Aon

+600

cyber claims handled since 2012

+200

cyber analytics projects

+\$600m

total cyber premium placed in 2018

Certified
cyber security
technical teams



CBEST



Recognised
industry leaders



FORRESTER

Forbes

What's your cyber defence?

Q&A

iapf 
representing pension savers

THANK YOU
Vanessa Jaeger and Karl Curran

iapf 
representing pension savers

THANK YOU DELEGATES

Please fill in the yellow evaluation form
CPD confirmation by email
Download presentation at
www.iapf.ie

iapf   
representing pension savers