NEW STRATEGIES AND RISKS

Prepared by Aon Risk Solutions

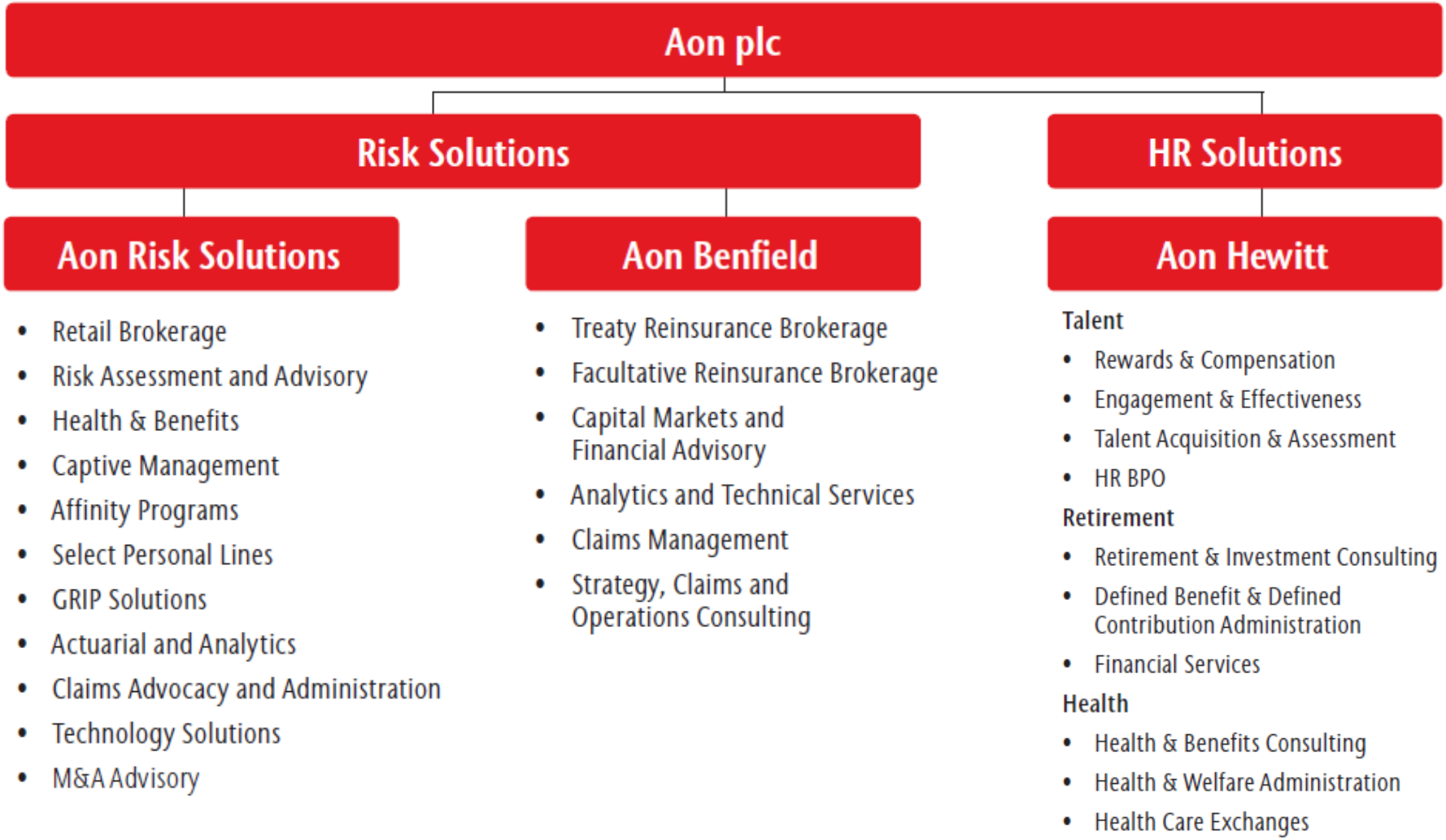
Empower Results®

Empower Results®

Beauty in Numbers

#1	Rated risk services broker, reinsurance intermediary, and human resource consulting and outsourcing provider
66,000	Number of Aon colleagues around the world
500	Number of global offices
120	Number of countries in which Aon operates
USD 12.0B	Total revenue generated by Aon in 2014

Aon Corporation



That is Risk ?

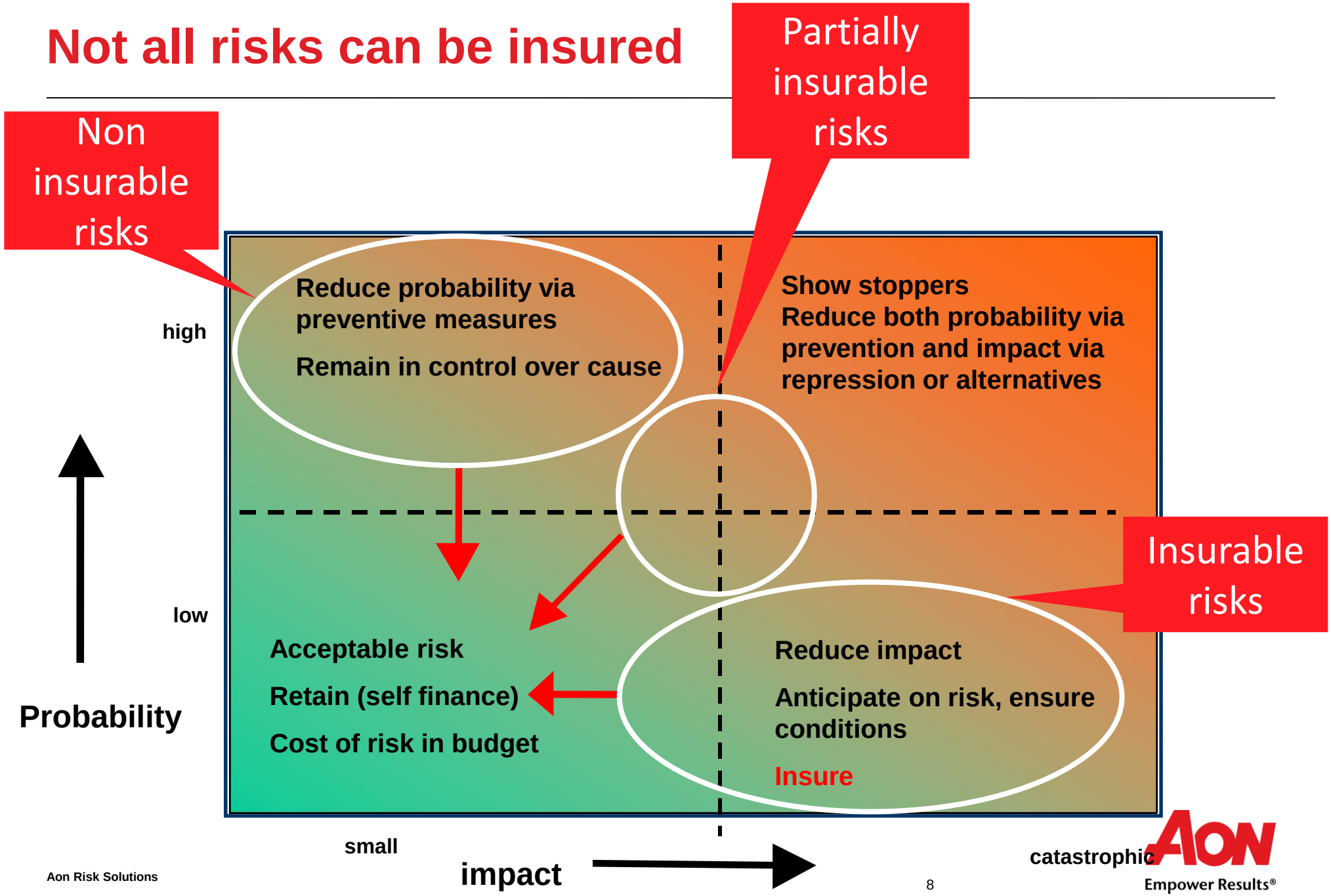
Risk

A Probability or threat of negative occurrence that is caused by external or internal vulnerabilities

Consequences…

Risk and Insurance

Not all risks can be insured



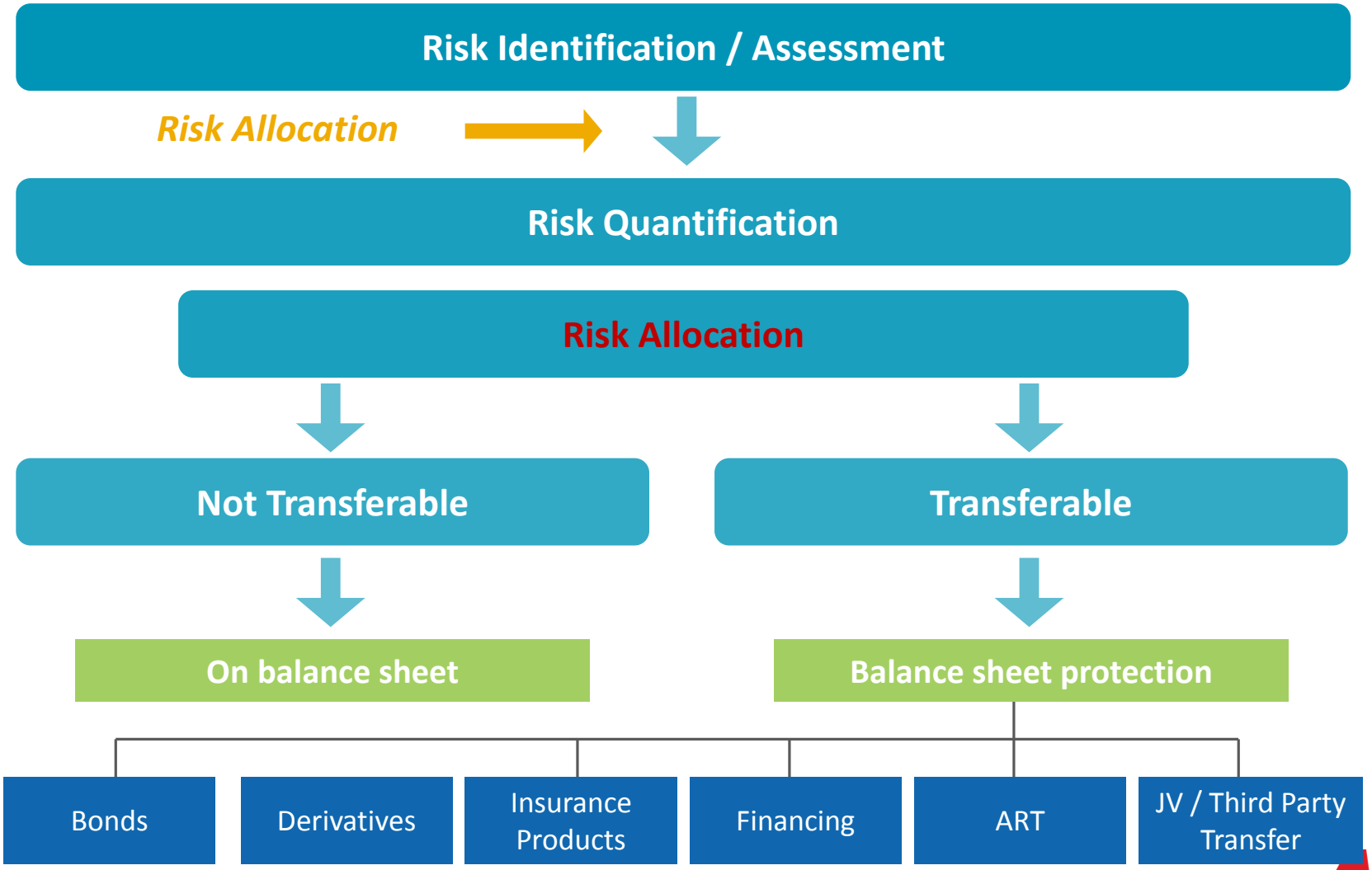
Top Risks according to Aon Global Risk Management Survey

1) Economic slowdown
2) Regulatory / legislative changes
3) Increasing competition
4) Damage to reputation / brand
5) Failure to attract or retain top talent
6) Failure to innovate / meet costumers needs
7) Business interruption
8) Commodity price risk
9) Cash flow/ liquidity risk
10) Political risk / uncertainty

Top Risks according to Aon Global Risk Management Survey

11) Exchange rate fluctuation
12) Technology failure / system failure
13) Third party liability
14) Distribution or supply chain failure
15) Capital availability/credit risk
16) Weather / natural disasters
17) Property damage
18) Computer crime / Hacking / viruses
19) Growing burden and consequences of corporate governance / compliance
20) Counter party credit risk

Risk Management



Risk Identification / Assessment

- D&O Insurance
- Trade credit insurance
- Business Interruption Insurance
- *CRIME* Insurance
- Travel insurance
- Employers liability
- *Cyber* Insurance

Cyber risk insurance

When should organizations be concerned about their cyber risk exposure?

Organizations should be concerned about cyber risk if they:

- Gather, maintain, disseminate or store private information
- Have a high degree of dependency on electronic processes or computer networks
- Engage vendors, independent contractors or additional service providers
- Are subject to regulatory statutes
- Are required to comply with PCI Security Standards/Plastic Card Security statutes
- Are concerned about contingent bodily injury and property damage that may result from cyber incidents
- Rely on or operate critical infrastructure (Personally Identifiable Information risk are less prominent for industries such as utilities, manufacturing and logistics)
- Are concerned about intentional acts by rogue employees
- Are a public company subject to the SEC Cyber Disclosure Guidance of 2011

Why are standard insurance policies not enough?

While existing forms sometimes carry a level of coverage, they were not intended to cover many risks associated with an increasingly digital world. Typical forms respond as follows:

- **General Liability:** covers bodily injury and property damage, not economic loss
- **Errors & Omissions:** covers economic damages resulting from a failure of defined services only, and may contain exclusions for data and privacy breaches
- **Property Insurance:** covers tangible property, which data is not. Loss must be caused by a physical peril while perils to data are viruses and hackers
- **Crime:** covers employees and generally only money, securities and tangible property. No coverage for third party property such as customer/client data

What is the scope of today's cyber coverage?

3rd Party Coverage

- • Wrongful disclosure of Personally Identifiable Information, Protected Health Information or confidential corporate information in the client's care, custody or control via a computer network or off-line (e.g., via laptop, paper, records, disks)
- • Failure of computer network security to guard against threats such as hackers, viruses, worms, Trojan horses and denial of service attacks whether or not resulting from the provision of professional services
- • Content liability perils such as defamation and infringement of intellectual property rights arising out of website, marketing and advertising activities
- • Security or privacy breach regulatory proceedings (including associated fines and penalties)

What is the scope of today's cyber coverage?

1st Party Coverage

- Network business interruption: loss of income and extra expense due to network security failure
- Intangible property: costs to restore or recreate data or software resulting from network security failure
- Breach response/management costs associated with:

– Breach notification, including the hiring of outside law firms and public relations consultants

– Credit monitoring/protection

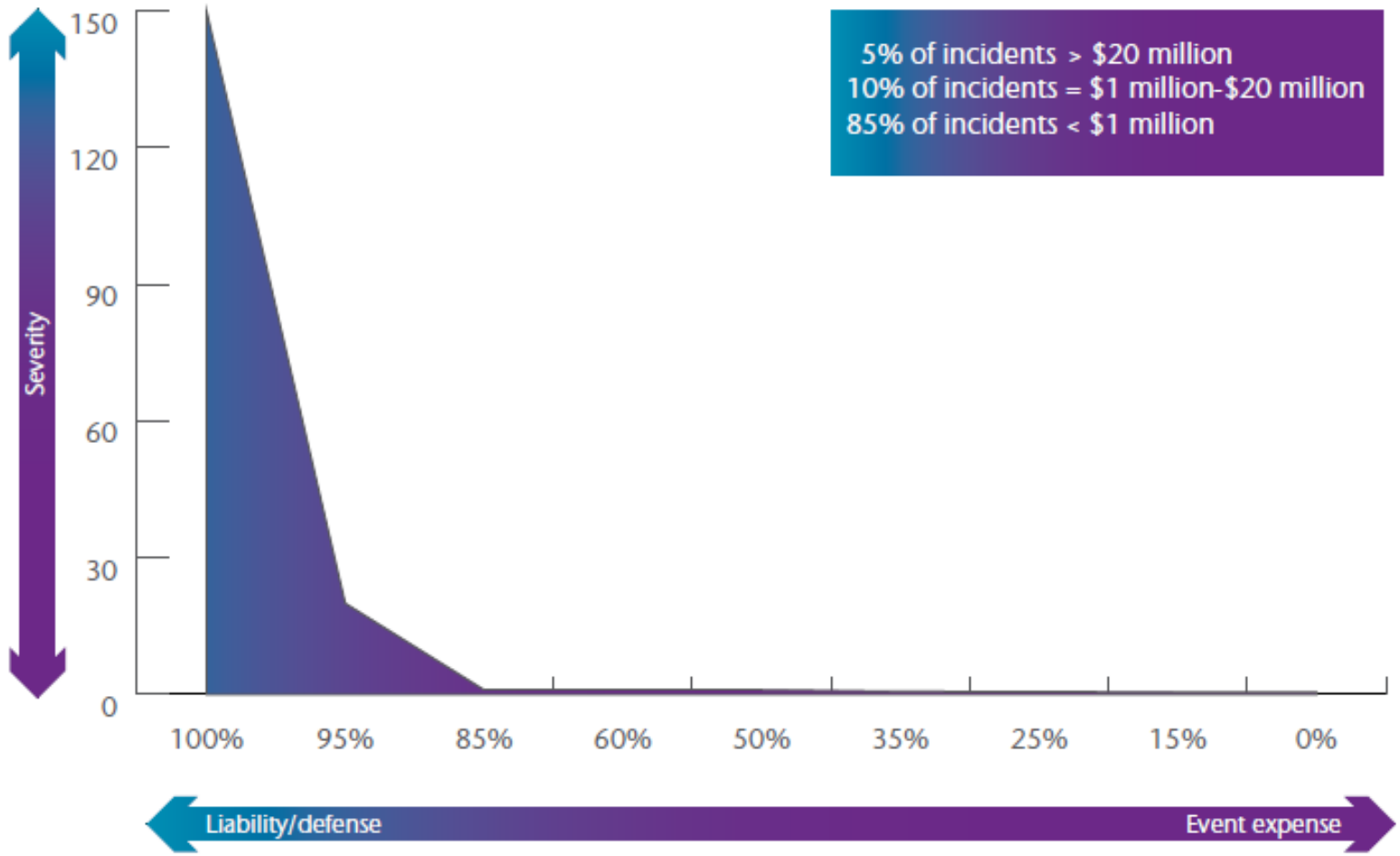
– Notification hot-line/call center

– Forensic costs

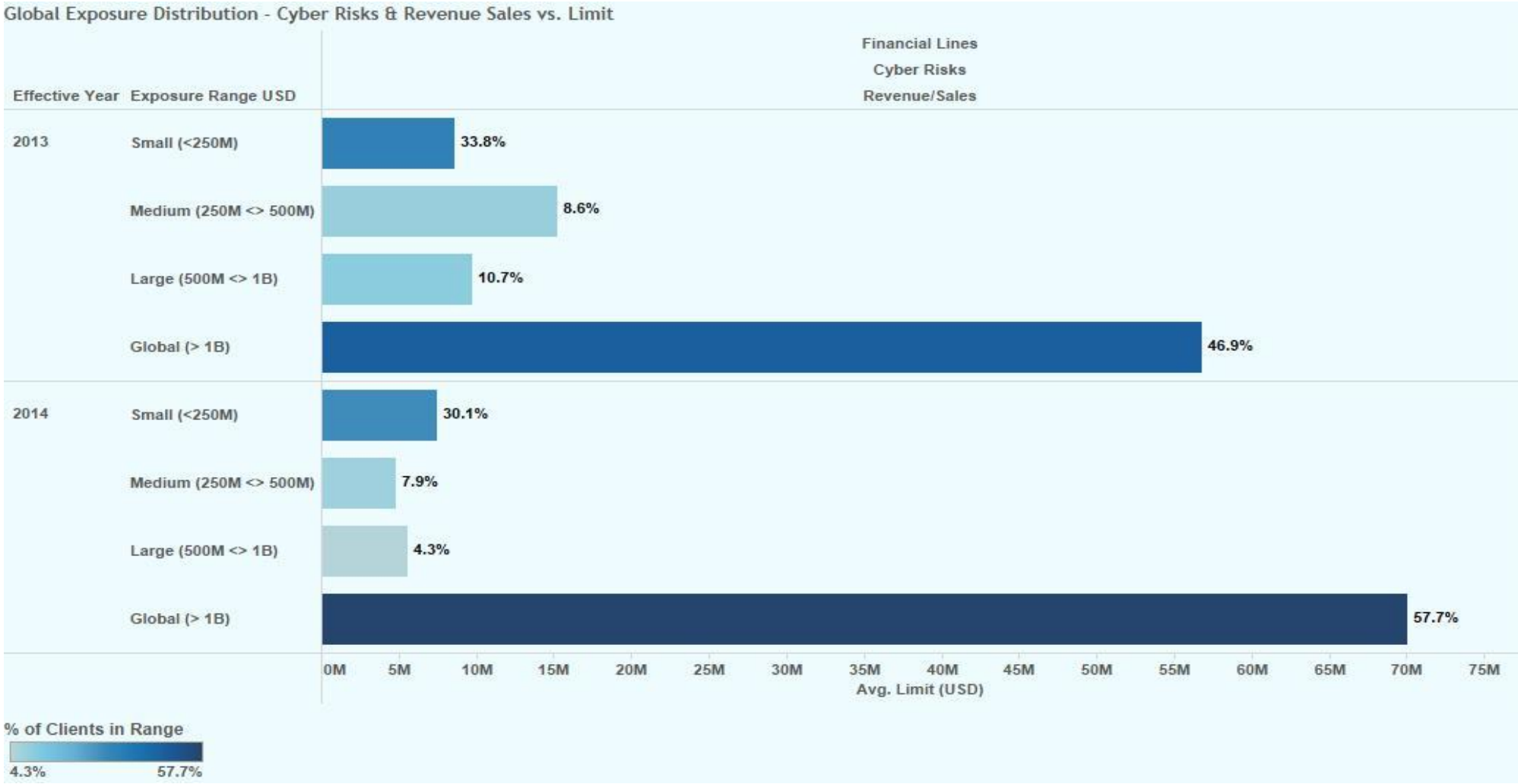
– Identity theft resources

- Cyber extortion
- Loss of income due to failure of network security

Cover and Gap analysis under existing policies



Exposure Distribution vs. Avg. Limits



www.aoncyberdiagnostic.com

English

Cyber Risk Diagnostic Tool

How exposed are you to cyber risks?
What influences your level of exposure?
Find out by taking our 15 minute diagnostic.

Aon's Cyber Risk Diagnostic Tool will help you identify the key internal and external factors that may affect your level of exposure to cyber risks. It will also give you real insight into the relevant cyber risk drivers, and provide you with practical guidance on a governance framework that you can put in place as part of an effective cyber risk management strategy.

Please reach out to your local Aon office to discuss your report or for specific advice.

Spend 15 minutes completing our diagnostic, and upon completion you will receive:

- A report highlighting your key cyber risk issues
- A visual indication and high level rating for your identified cyber risks
- Practical advice on putting in place an effective cyber risk management strategy

Start your diagnosis

Contact Details

Aigars Milts | Country Manager

Aon Baltic Latvian Branch

Biekensalas street 6 | Riga| Latvia

t. +371 6 789 2551 | m. +371 2 938 9194

e-mail: aigars.milts@aon.lv