Institute and Faculty of Actuaries

Cyber Risk For Insurers

Catastrophic impact or manageable operational risk?

Ramiz Mohamed

Contents

- Cyber Risk Working Party aims
- What type of cyber events are insurers exposed to?
- What is the potential size/extent of losses that could result for an insurer from a cyber risk event?
- Allocating cyber costs and timeline of losses
- What data sources are available to assist with measuring cyber risk?

Institute and Faculty of Actuaries

Cyber Risk Working Party

- Currently, cyber risk capital is held within insurers' operational risk capital as an implicit allowance. Given the growing size of the potential risk, it needs to be understood better.
- The Cyber Risk Working Party was set up to:
  - (1) Provide a resource base for actuaries to learn more about the operational risk faced by insurers, and the potential impact if a cyber event occurred in their company.
  - (2) Create a better measure of capital required, and risk mitigation steps available.
  - (3) Ensure the emerging threats and risk mitigation activities are understood by risk management actuaries.

Institute and Faculty of Actuaries

Types of cyber events affecting insurers

Event type	Description	Evidence	Examples
Actions of people	Intentional – fraud, theft, unauthorised activity Unintentional – human error	Causes 62% of all incidents ICO Q1 2016	Anthem data breach 2015
Systems and technology failures	Insufficient investment IT Deficiencies in data loss protection controls	ICO increase fines for IT systems failure	Staysure fine £175k for IT failure ICO 2015
Failed internal processes	Deficient governance Incompetence Non-compliance Business continuity plan	Some insurers x6 exposed to malware (Cisco 2015)	Accendo Insurance error 2011

Institute and Faculty of Actuaries

Potential size of losses

Case study – Anthem

American Health Insurance company with nearly $80bn global turnover, $2.56bn net income as at 2015

- Hackers gained access to over 80m personal data records
- First party costs alone reported to be well in excess of $100m
- Number of class action law suits have been filed
- E&O Tower reported to expect losses (no precedent for such claim yet)
- Government fines are highly likely
- Possible cost data breach? **Could be a significant % of global revenue!**

Institute and Faculty of Actuaries

Cyber Attack Costs - Allocation

Direct expenses result from the direct expense outlay to accomplish a given activity. These can include engaging forensic experts and other consultants, outsourcing hotline support and providing free credit monitoring subscriptions and discounts for future products and services.

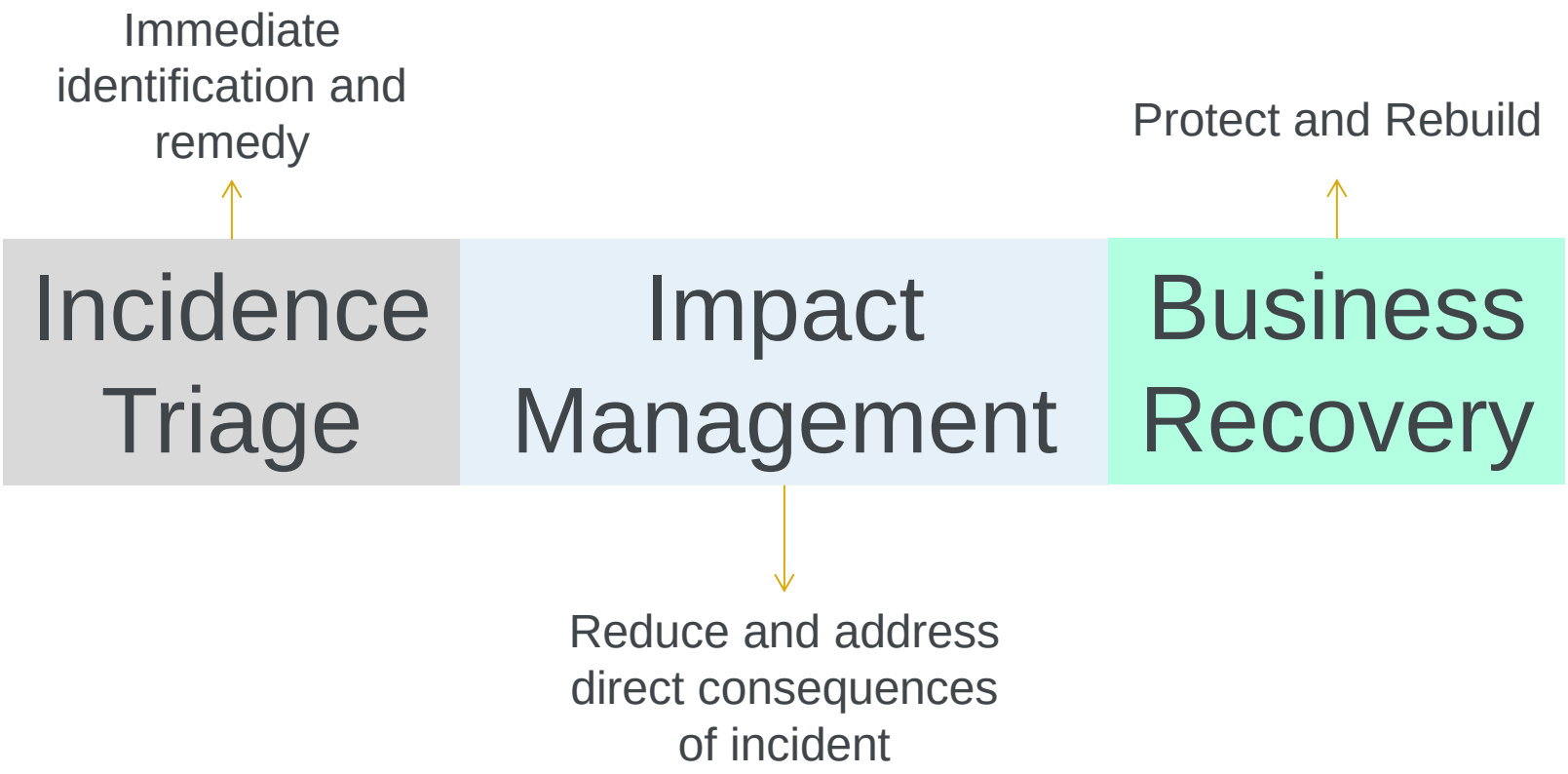
Indirect costs result from the amount of time, effort and other organisational resources spent, but not as a direct cash outlay. Examples include in house investigations and communication, as well as the extrapolated value of customer loss resulting from turnover or diminished customer acquisition rates.

Opportunity costs results in from diminished trust or confidence by present and future customers. Negative publicity associated with cyber incidences can cause reputational damage, that result in lower renewal rates, as well as a diminished rate for new customer acquisitions.

Source: Ponemon Institute

Institute and Faculty of Actuaries

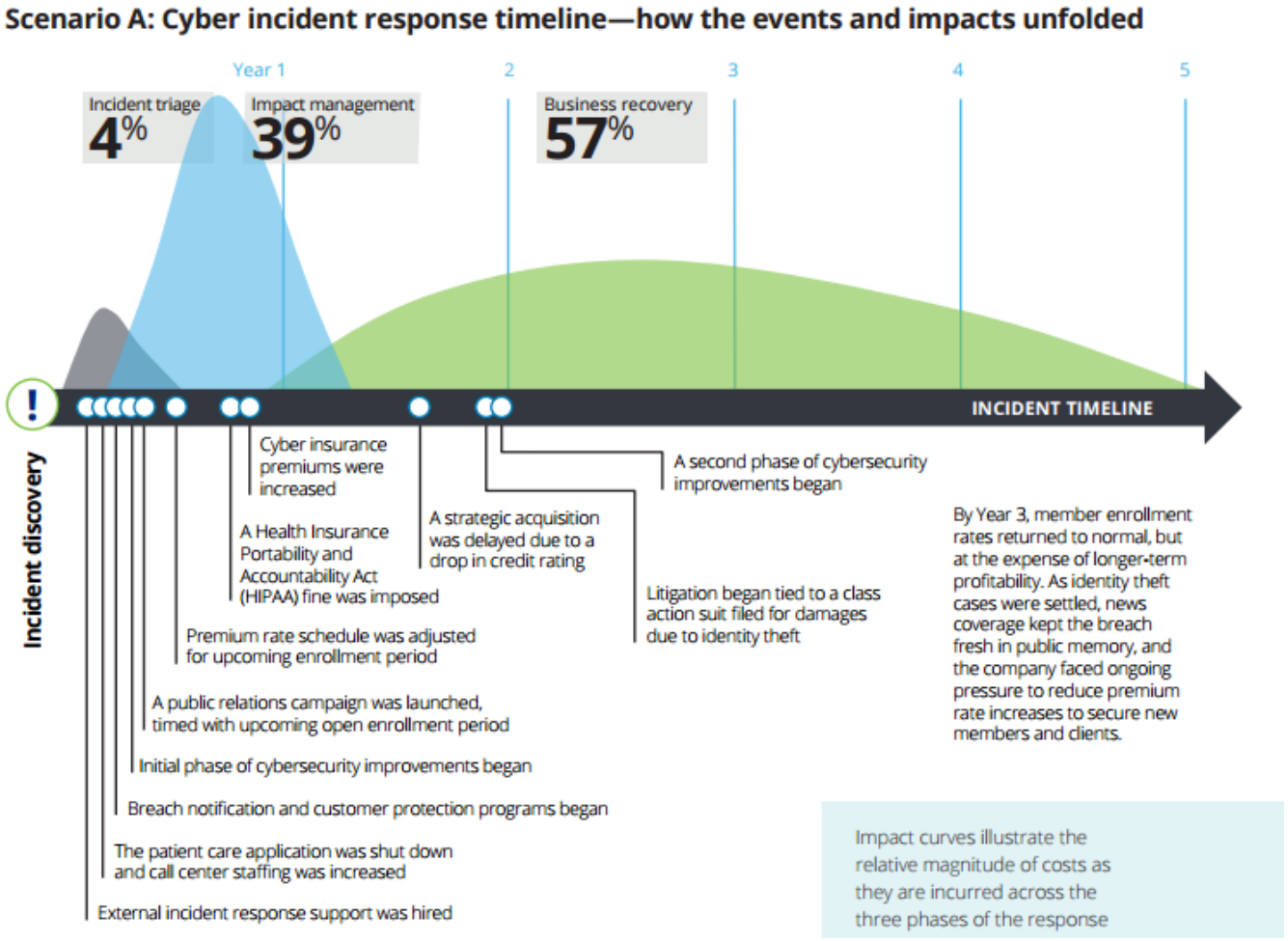
Cyber Attack Costs - Timeline



Source: Deloitte

Institute and Faculty of Actuaries

Cyber Attack Costs - Timeline



Source: Deloitte

Institute and Faculty of Actuaries

Cyber Attack Costs - Timeline

Summary of the impact factors

	Impact factor	Term	Cost (in millions)	% Total cost
Above the surface	Post-breach customer protection	3 years	21.00	1.25%
	Cybersecurity improvements	1 year	14.00	0.83%
	Customer breach notification	6 months	10.00	0.60%
	Attorney fees and litigation	5 years	10.00	0.60%
	Regulatory compliance (HIPAA fines)	1 year	2.00	0.12%
	Public relations	1 year	1.00	0.06%
	Technical investigation	6 weeks	1.00	0.06%
Beneath the surface	Value of lost contract revenue (premiums)	5 years	830.00	49.43%
	Lost value of customer relationships (members)	3 years	430.00	25.61%
	Devaluation of trade name	5 years	230.00	13.70%
	Increased cost to raise debt	5 years	60.00	3.57%
	Insurance premium increases	3 years	40.00	2.38%
	Operational disruption	Immediate	30.00	1.79%
	Loss of intellectual property	Not applicable	-	0.00%
	Total		**$1,679.00**	**100.00%**

Source: Deloitte

Institute and Faculty of Actuaries

Modelling Approach through Operational Risk

- Process Map
  - Benchmark on Industry Loss Data
  - Allow for some key drivers of risk
    - Revenue Size
    - Location
    - Insurance vs Other Financial Institutions
    - General (Commercial & Personal) vs Life
  - Allow for own companies specific risk characteristics
  - Size of tail?

Institute and Faculty of Actuaries

Cyber Risk Data

- Papers
  - Ponemon Institute
- Databases
  - ORX / ORIC
- Classifications
  - A Taxonomy of Operational Cyber Security Risks
- Scenarios
  - Cambridge Risk Framework

Institute and Faculty of Actuaries

Institute and Faculty of Actuaries

Cyber Risk For Insurers

Catastrophic impact or manageable operational risk?

Q&As

DISCLAIMER The views expressed in this presentation are those of the presenter and not necessarily of their employers.