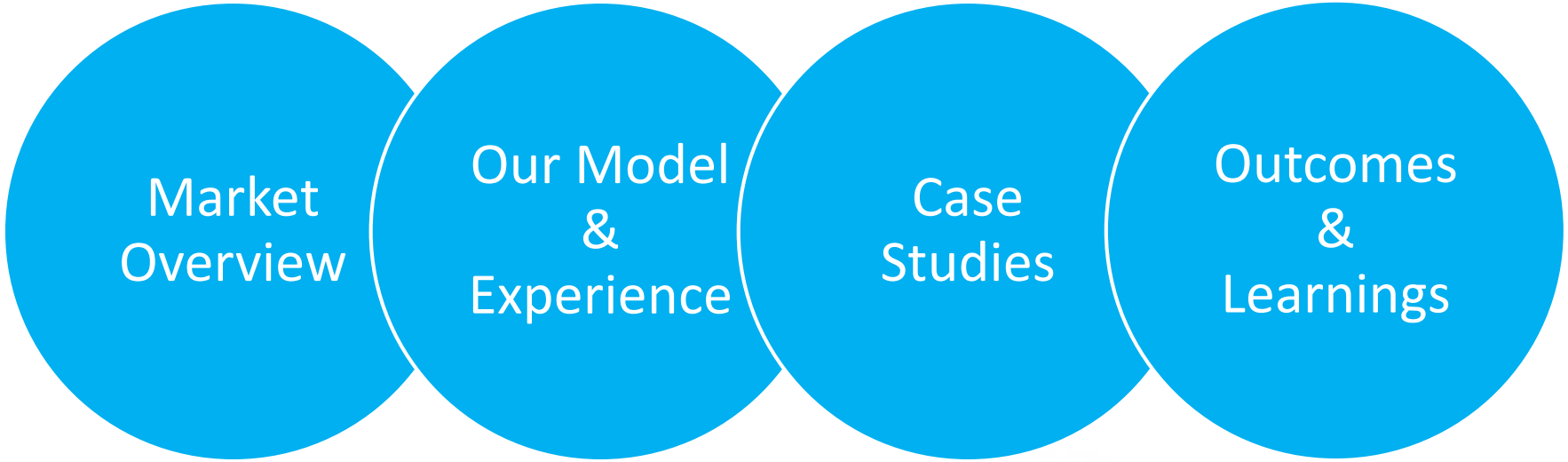
Global solutions.
Local expertise.

sedgwick®

Cyber Claims

Outline

Global solutions. Local expertise.



sedgwick®

CYBER INCIDENTS

- Video Major Cyber incidents 2018
- Video British Airways 2019

- TYPE OF ATTACK
  - MALWARE
  - RANSOMWARE
  - PHISHING
  - MAN IN THE MIDDLE
  - DENIAL OF SERVICE (DDOS)
  - ZERO DAY EXPLOITS

- EXPLANATION
  - MALICIOUS SOFTWARE
  - BLACKMAIL TOOL
  - EMAILS CONTAINING MALICIOUS CODES
  - ATTACKS BETWEEN TWO COMM. USERS
  - INUNDATES SERVERS WITH TRAFFIC
  - MALWARE THROUGH VULNERABILTIES OF NEW SOFTWARE

sedgwick®

l solutions. Local expertise.

THE ETERNAL CYCLE OF HIGH-PROFILE DATA BREACH

SenseCy
Sensing Cyber

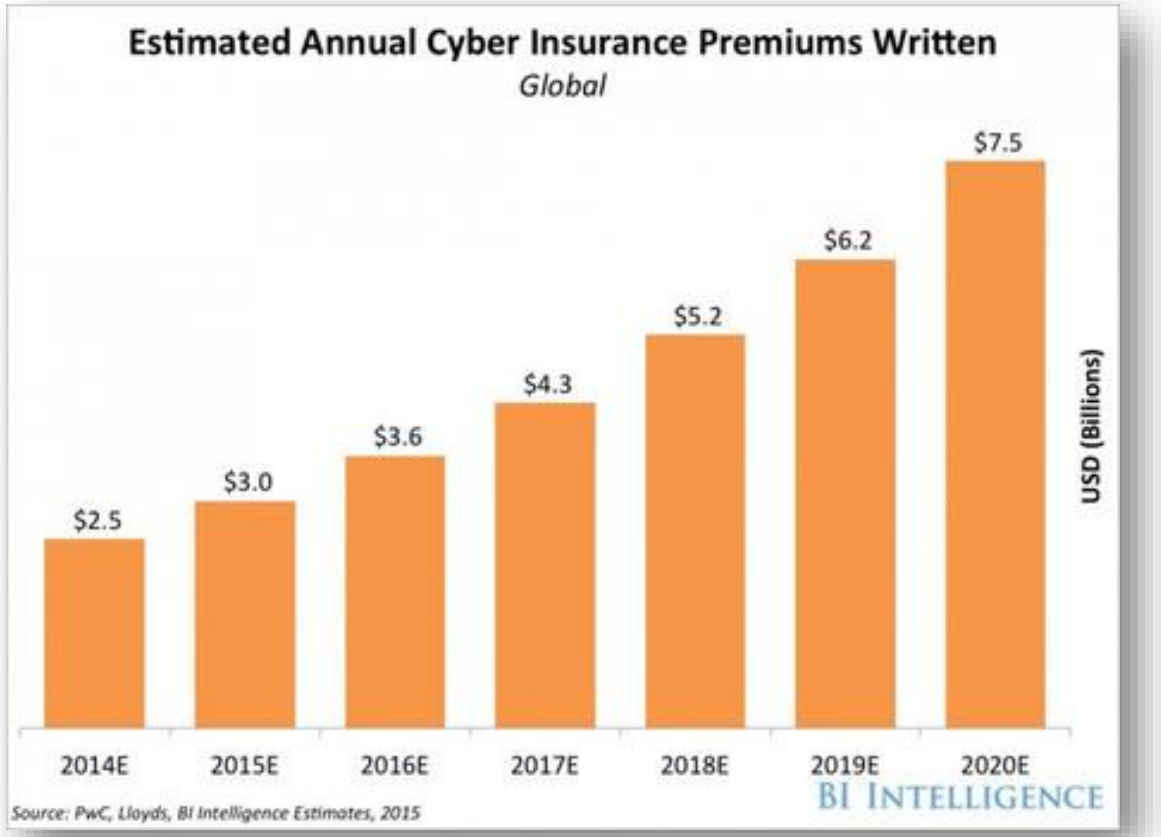
sedgwick®

Cyber Insurance: Global

Global solutions. Local expertise.

Global market

- Cyber products have been around since the late 1990s
- Infancy of market, emerging needs and evolving products
- It is estimated that premiums from the global market will grow to $7.5 billion by 2022
- The cost to the global economy is more than $400 billion a year and continues to grow



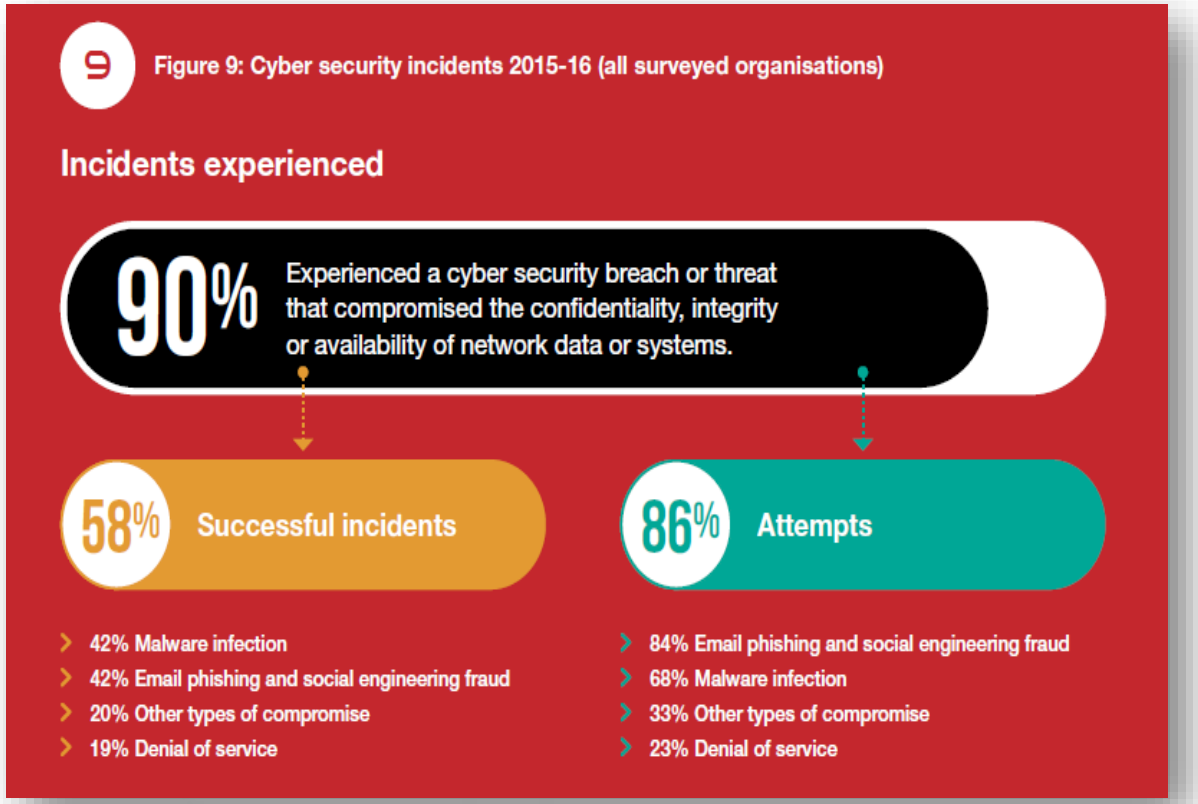
sedgwick

Cyber Insurance: ASIA

Global solutions. Local expertise.

ASIA market

- Buyers mainly in the Telco, Technology and Financial Centers
- SME's buyers have yet to come to the party
- More customers buying BI extensions
- Market size of approx. $100m - 2019
- Cover led by major Reinsurers, Chubb, AIG, Munich Re
- Stand alone and add-on policies

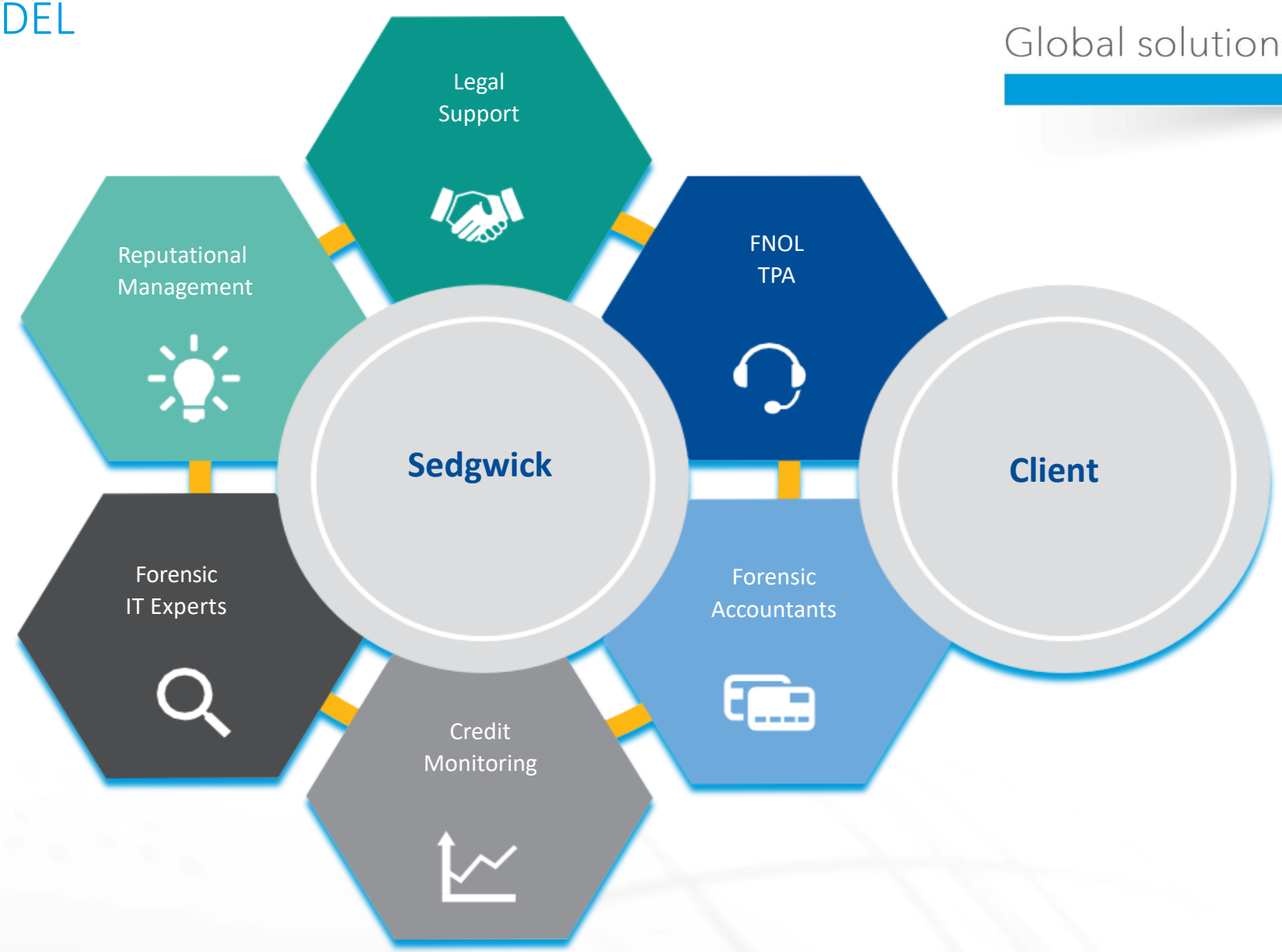


Source: ACSC 2016 Cyber Security Survey

sedgwick

CLAIMS MODEL

Global solutions. Local expertise.



sedgwick

Sedgwick Claims Experience

Global solutions. Local expertise.

Global footprint & > 1000 cyber claims

UK, Asia, Australia, New Zealand

- 14+ clients
- 40FTE team
- GDPR, NDB privacy breaches
- Decryptions
- Claim Types:
  - SME
  - Enterprise
  - High Net Worth
  - Personal Lines
- Industry Awards

Munich RE
Munich Reinsurance Company of Africa Limited (MRoA)
Alm Brand
CONSORT
YOUR TRUSTED INSURANCE ADVISORS
KingPrice INSURANCE
1866
HSB Engineering Insurance
uk general
ERGO
DAS
Ecclesiastical
NIG
AXA
COvea Insurance
cfc
EMERGENCE
Plum UNDERWRITING
Liberty Insurance
N1 CYBER INSURANCE
STERLING looking after tomorrow
CHUBB
DELTA INSURANCE
vero liability
sedgwick

What do claims look like?

Global solutions. Local expertise.

sedgwick

CLAIMS VIDEO

- BBC news – one ransomware

Cyber Claim Lifecycle

Global solutions. Local expertise.

The first 48 hours are key

FNOL

- 24/7 hotline
- Incident manager contacts Insured
- Notify Insurer, Broker

1st 12 Hours

- Triage call with Insured, experts
- Containment, mitigation measures
- Review Policy coverage
- Clear Discovery Next Steps

Next 12 Hours

- Containment, mitigation efforts
- Engage Insurer, broker
- Stakeholder updates

Within 48 hours

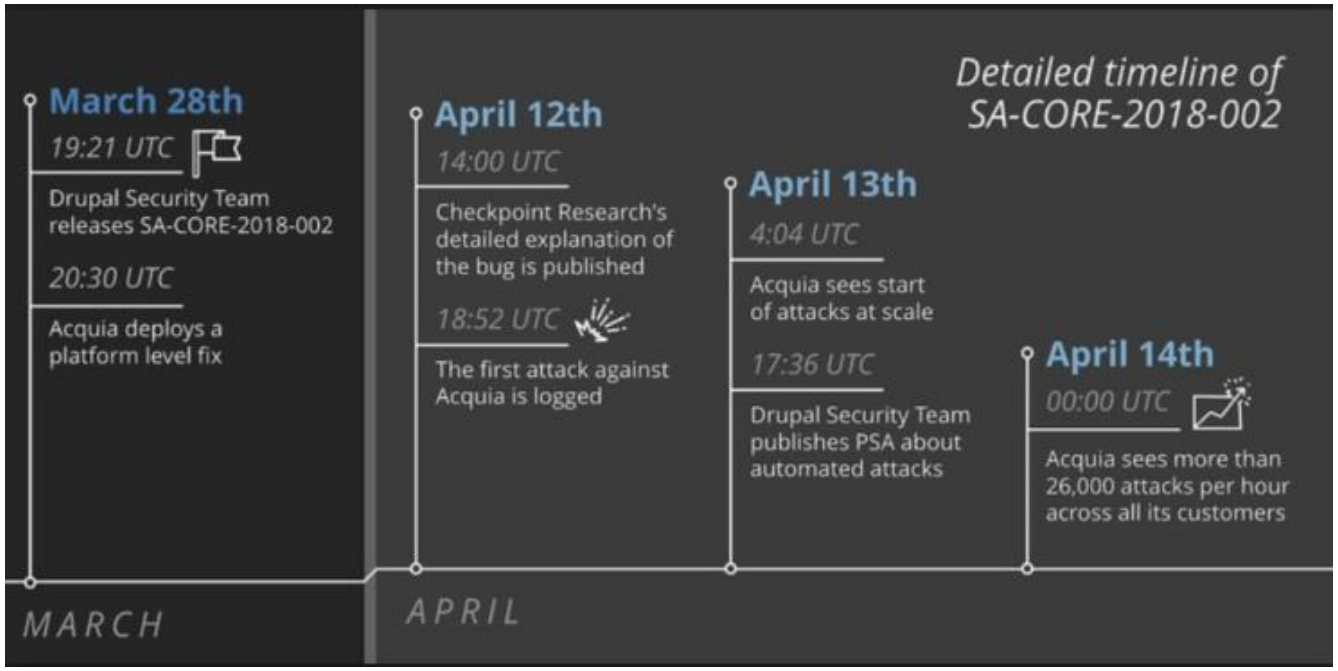
- Clear Solution next steps emerge
- Rectification plan
- Notify regulator, legal representation?
- PR required?
- Business interruption?

- Proactive timely response to contain immediate impact and mitigate future losses
- Intense broker, insurer, insured engagement
- Ensure confidentiality and protect privilege
- Consistent and professional claims management approach

sedgwick®

Case Study – Website Hack

Global solutions. Local expertise.



Event

- **Website was hacked**
- **Threat of crypto locker – 'Drupalgeddon 2'**
- **Bitcoin ransom demanded for decryption key**

Remediation/Action

- Website immediately taken offline
- External IT specialist engaged
- Call centre established to handle all queries
- Loss Adjuster and Lawyer appointed

Issues

- NDB obligations
- 3rd party IT agreement
- Ransomware – to pay or not to pay?
- PR & Media – insuring more than Cyber breach

Outcome

- Almost 3 months to restore website
- Indemnity granted – restoration and incident response costs

sedgwick

Case Study – Small Phish

Global solutions. Local expertise.

First 48 hours translated

Monday

11:45am: Malicious email received
12:15pm: Insured clicks on link to the proposal

Tuesday

Hacker has gained control of Insured's email, downloads inbox (folders sync) and changes auto forwarding rules

Wednesday

~10am: Hacker starts sending out phishing emails
2pm: IT Vendor receives email, notifies Insured, resets password
3:30pm: Notifies incident response line
4:30pm: Stakeholder Call
6pm: Email to all clients to ignore the email sent earlier
6pm: Engages MS Admin to delete hidden auto forwarding rules to deleted inbox

Thursday

8am: IT Forensics continues – no auditing logs enable, RDS Server malware scan
9am: Process begins to analyse information stored in Insured's inbox

Friday

Insured operating normally and continues to analyse inbox

sedgwick

Cyber Claims – Incident Response

Global solutions. Local expertise.

Case Study Learnings

- Incident response time to react – internal, external IT, objectives
- Ransoms – to pay or not to pay
- Decryption services – cost effective, worth it?
- Recoveries – vendor agreements
- Exclusions: Betterment, Social engineering, Proprietary information

sedgwick®

Cyber Claims – Business Interruption

Global solutions. Local expertise.

Case Study Learnings

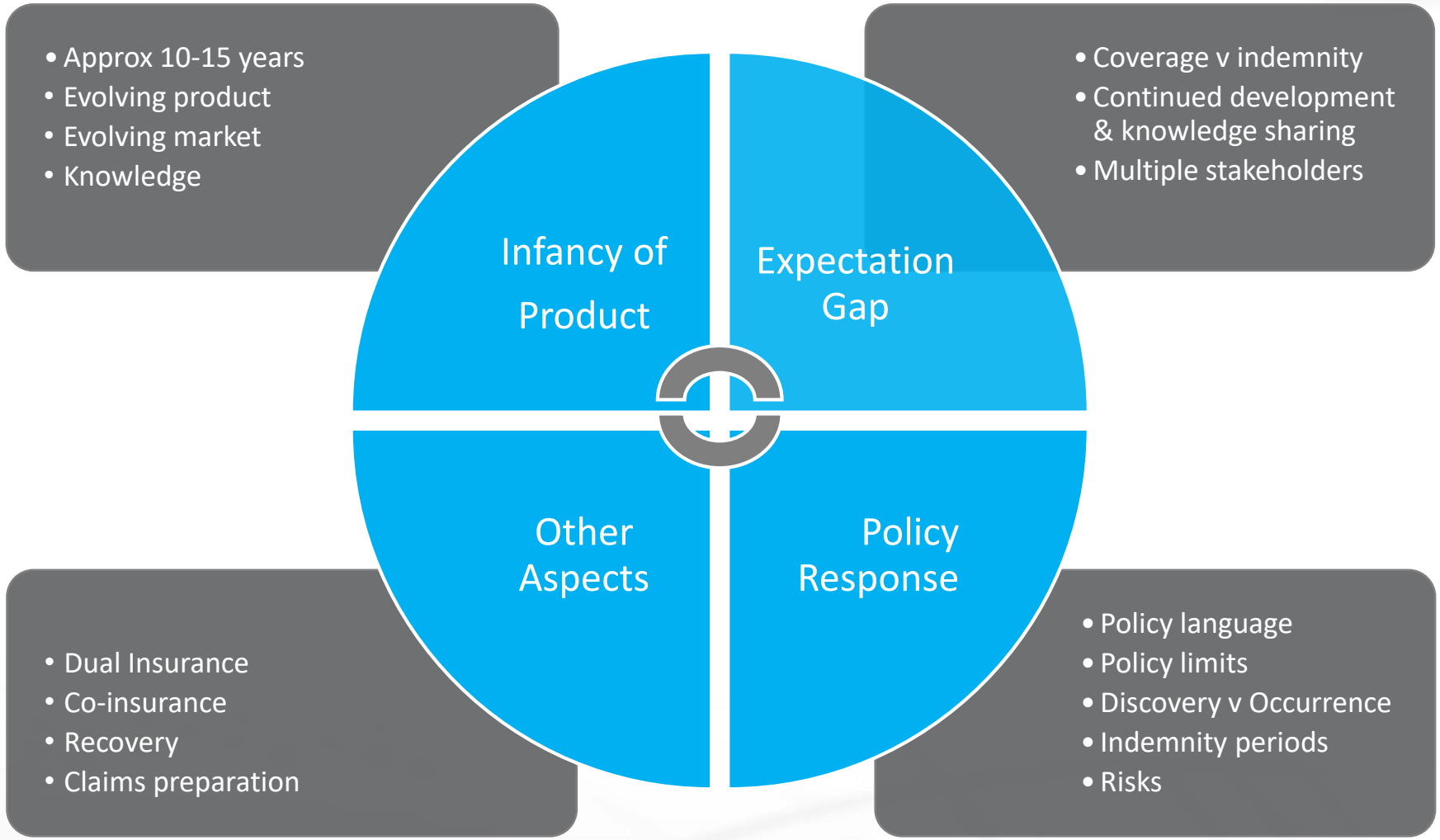
Understand the revenue drivers of a business. How is revenue recognised and recorded

- Indemnity periods – move is to shorter indemnity periods, select period that coincides with operating cycle
- Excesses – time and monetary deductibles
- Extensions – contingent BI
- Exclusions – internal resources vs 3rd party, normal expenses vs additional costs, inconvenience vs actual losses
- Specific Industries – retail, online, professional services

sedgwick

Key Outcomes and Learnings

Global solutions. Local expertise.



sedgwick®

Q&A