GUY CARPENTER

INTRODUCTION TO CYBER (RE)INSURANCE

May 2018

MARSH & McLENNAN COMPANIES

Agenda

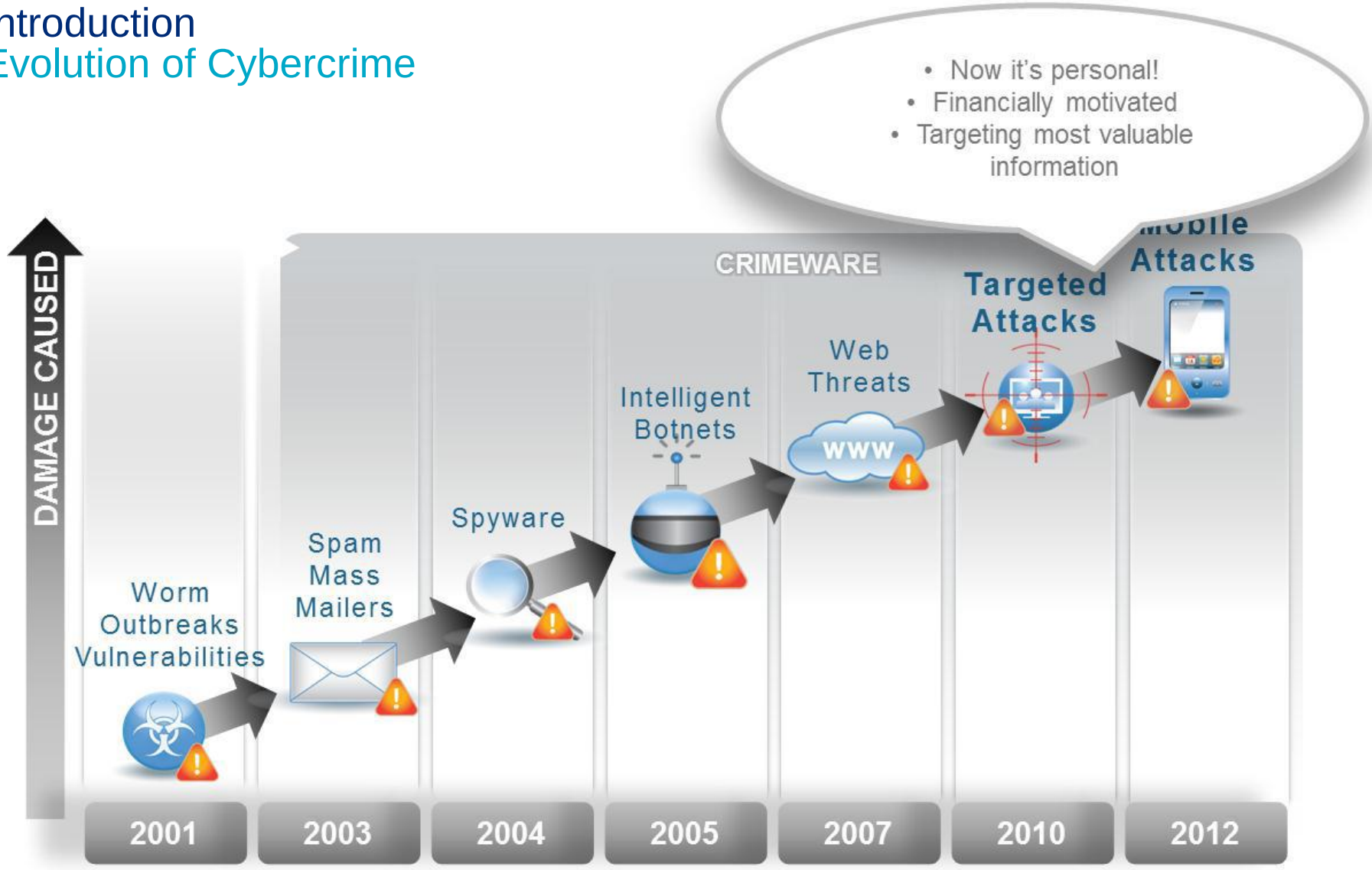
1) Introduction – What is Cyber?
2) Difference between the US and Europe
3) Cyber Risk in APAC
4) Industry Research and Model
5) Model Data Input and Output
6) Underwriting Coverage
7) Cyber Claims

1. Introduction – What is Cyber?

Introduction
What is Cyber (Re)insurance?

- The development of information technology and online connectivity has changed the way businesses operate. ‘Big data’ and intricate IT systems are vital to today’s economy. Cyber insurance has grown out of recognition that cyber-crime and data privacy are amongst the most concerning risks facing organisations today.
- ‘Cyber’ is perhaps a misleading term to describe the type of cover offered. The term describes a number of coverages for an organisation’s computer system, data and other multimedia activities. These covers are typically designed to include the following:
    - Data breach and privacy crisis management
    - Multimedia Activities and Media Liability
    - Network Security Liability
    - First party losses – data damage, extortion and business interruption
- Cyber insurance as a product has its origins in the Technology E&O market before gradually evolving into a separate cover in its own right.

Introduction
Evolution of Cybercrime



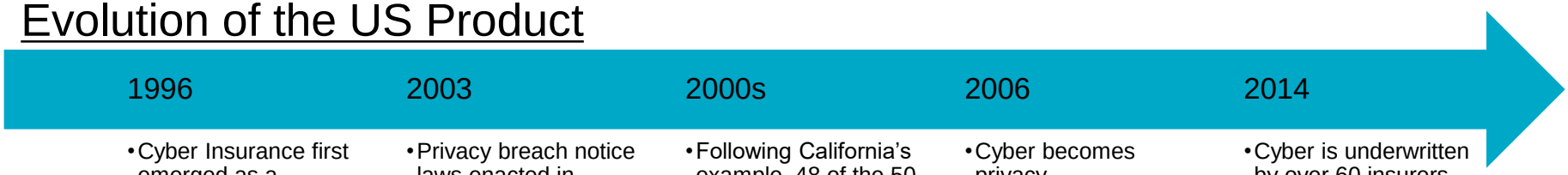
Source: Trend Micro Inc

2. Difference between the US and Europe

Introduction

Historical Development of Cyber (Re)Insurance - How has this product evolved over time?

Evolution of the US Product



1996
- Cyber Insurance first emerged as a product.

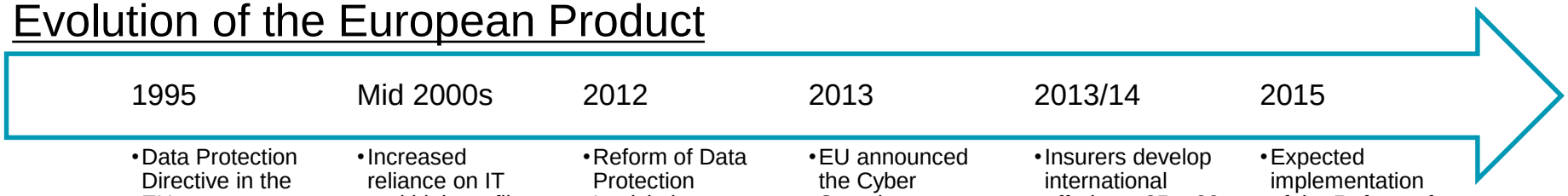
2003
- Privacy breach notice laws enacted in California, furthering demand for Cyber products

2000s
- Following California's example, 48 of the 50 states have now enacted compulsory breach notification legislation, driving the Cyber market in the US

2006
- Cyber becomes privacy

2014
- Cyber is underwritten by over 60 insurers and produces over $1bn a year in premium income

Evolution of the European Product



1995
- Data Protection Directive in the EU.
- Established data protection as a right for EU citizens

Mid 2000s
- Increased reliance on IT and high-profile hacking scandals lead to increase in enquiries for cyber insurance in Europe.

2012
- Reform of Data Protection Legislation released by the EU. This detailed compulsory breach notification rules, increases in fines to be enforced and other requirements for data protection.

2013
- EU announced the Cyber Security Directive, which will impose minimum security measures on businesses.

2013/14
- Insurers develop international offerings. 25 – 30 markets in London

2015
- Expected implementation of the Reform of Data Protection Legislation. (However, this date is a moving target).

Difference between the US and Europe
How does cyber coverage vary between the regions?

In the US, there is no all-encompassing federal legislation regulating data protection and individual privacy.

Each state has their own laws. The complexity of legislation combined with mandatory breach notice laws introduces opportunities for class action as well as punitive actions by regulatory bodies, State AG's and the Federal Trade Commission.

This means that **data privacy** is the focus of Cyber.

In Europe, data is viewed as human right and comprehensive regulation exists to protect the individual's data and privacy.

The collection and purpose of data is subject to strict conditions but with limited (€600,000) monetary sanctions, no compulsory notification of data subjects and no tradition of class action.

For European organisations, the **Business Interruption** element **(First Party)** is of at least equal importance as the Cyber coverage.

PII vs. PHI vs. PCI
Black Market Prices of Stolen Digital Assets

Digital Asset	2012	2015
Healthcare Record	$5	$15
Bank Account Access Credentials	$3	10
US Credit Card Number	$1	$0.5
Credit History	$0.24	$0.39
PayPal Account Access Credentials	$0.15	$0.25
eBay Account Access Credentials	$0.12	$0.2
Social Security Number	$0.5	$0.1
Email Access Credentials	$0.002	$0.0002
Name, Address, Email Address, Phone No.	$0.001	$0
	Percentage of face value	
CryptoCurrencies (BitCoin etc.)	30%	35%
Loyalty Program Rewards (Airmiles, Supermarket points)	20%	25%
Physical Goods for Sale	10%	12%
Pre-paid Call Minutes	8%	8%

Source: RMS: Managing Cyber Insurance Accumulation Risk

Mandatory Breach Notice Law
Example using California

- California was the first of 48 U.S. States with security breach notification laws. It became effective July 1, 2003.
- Requires notification to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
- Corporations can determine whether they are subject to this statute by reviewing the following questions:
  - Does their data include "personal information" as defined by the statute?
  - Does that "personal information" relate to a California resident?
  - Was the "personal information" unencrypted?
  - Was there a "breach of the security" of the data as defined by the statute?
  - Was the "personal information" acquired, or is reasonably believed to have been acquired, by an unauthorized person?
- A corporation that answers yes to all five of these questions must report.
- The statute does not apply to "encrypted" information.
- "Personal information" means an individual's name in combination with any of the following:
  - Social security number.
  - Driver's license number or California Identification Card number.
  - Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Reform of the EU Data Protection Legislation
What are the proposed EU regulations?

A 72-hour compulsory notification period

- Must notify the data regulator without “undue delay” and “where feasible” within 72 hours of a breach

Huge potential fines

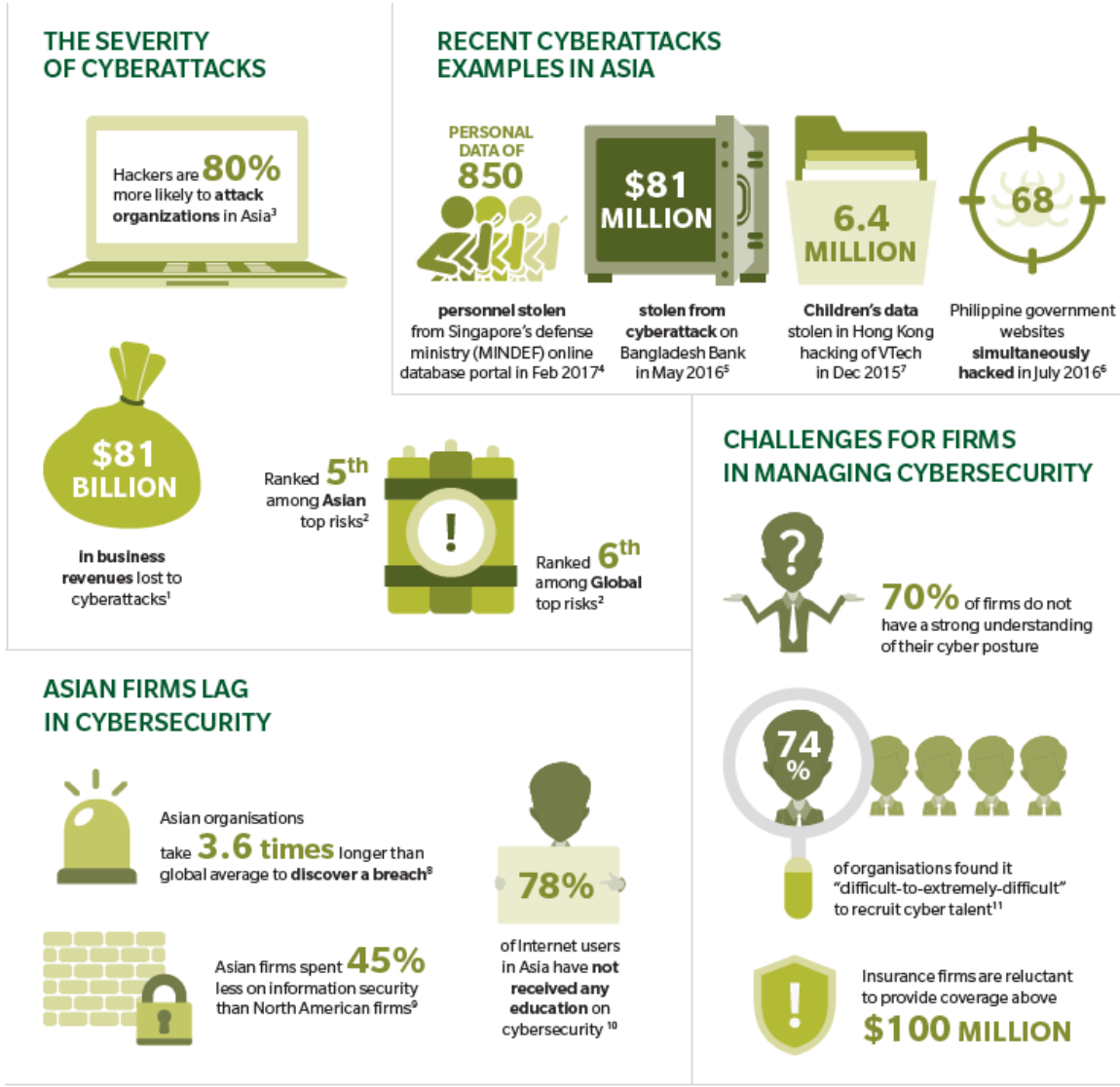
- Fines of up to €20M or 4% of annual turnover

The appointment of a dedicated position of data protection officer

- For organisations that process more than 5,000 data subjects in a 12 month period
- Must act as an independent assessor of compliance, even when the handling of customer data is outsourced to third parties

3. Cyber Risk in APAC

Cyber Risk in APAC
Risk in Numbers

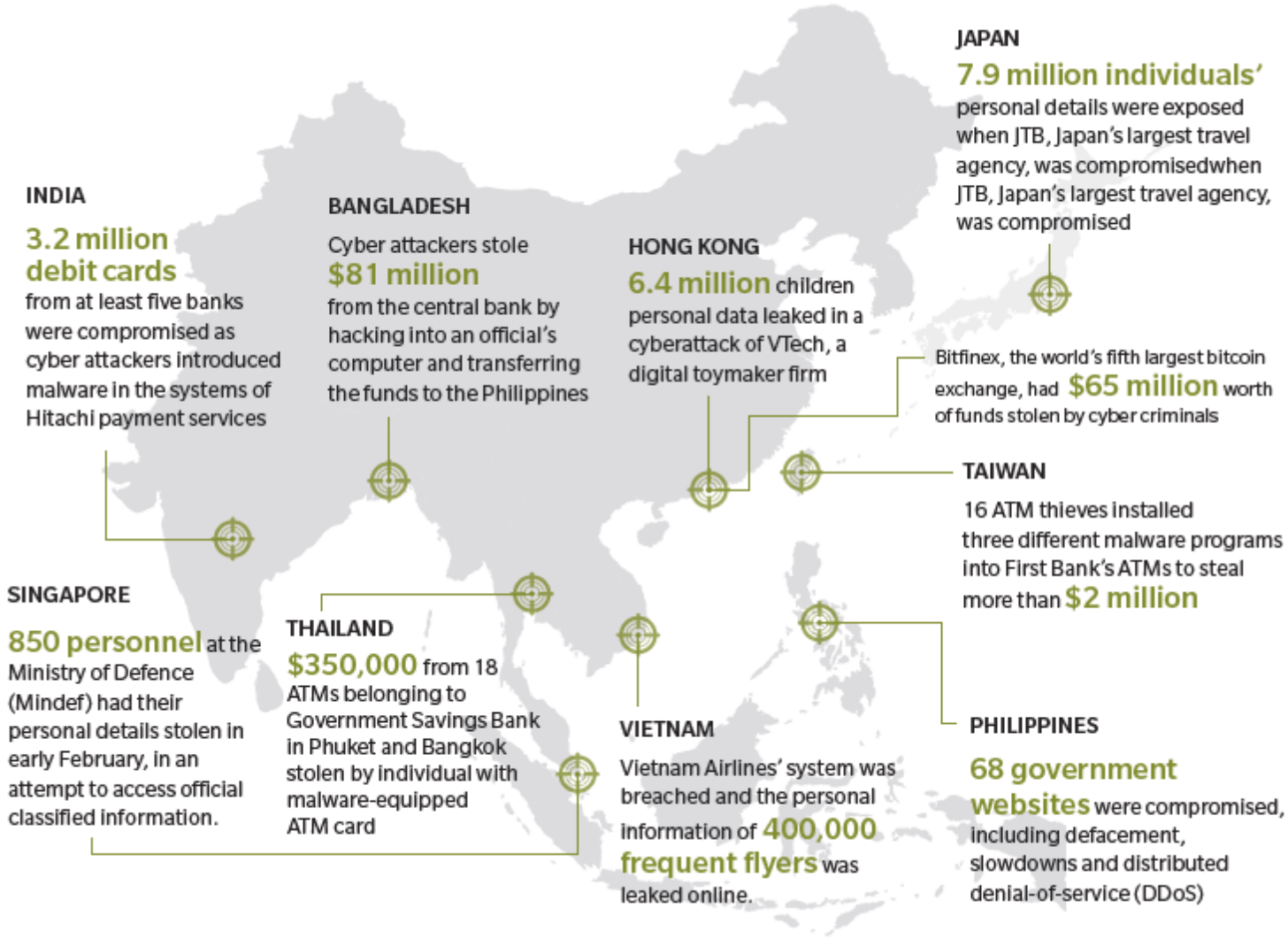


Source: MMC: Cyber Risk in ASIA-Pacific

APAC cyber risk

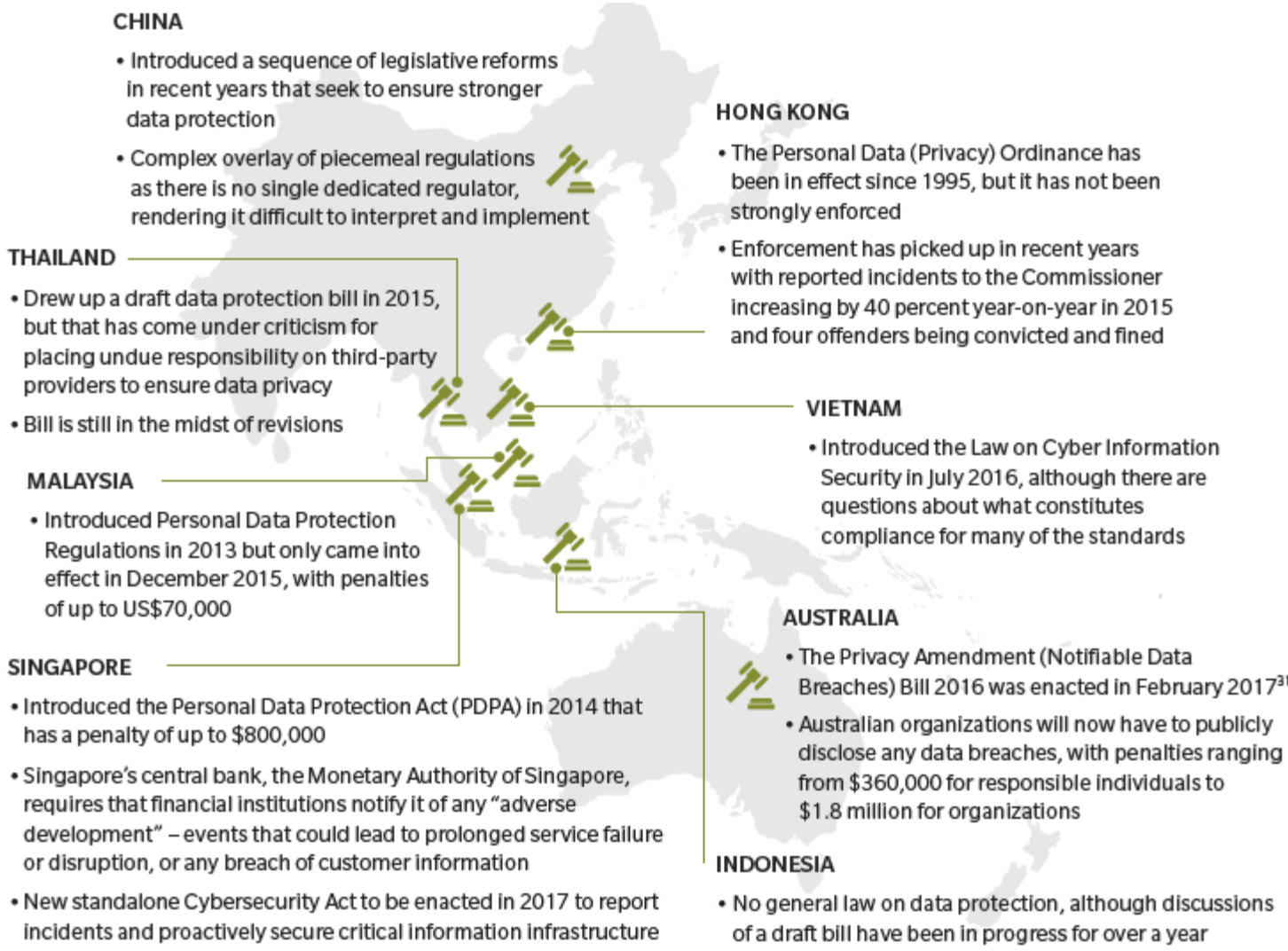
- higher attack frequency
- higher vulnerability
- less budget in cyber security

Cyber Risk in APAC
Cyberattacks in APAC – Tip of the iceberg?



Source: MMC: Cyber Risk in ASIA-Pacific

Cyber Risk in APAC
Developments in data privacy regulations



Source: MMC: Cyber Risk in ASIA-Pacific

Cyber Risk in APAC
Cyber (Re) Insurance in Australia

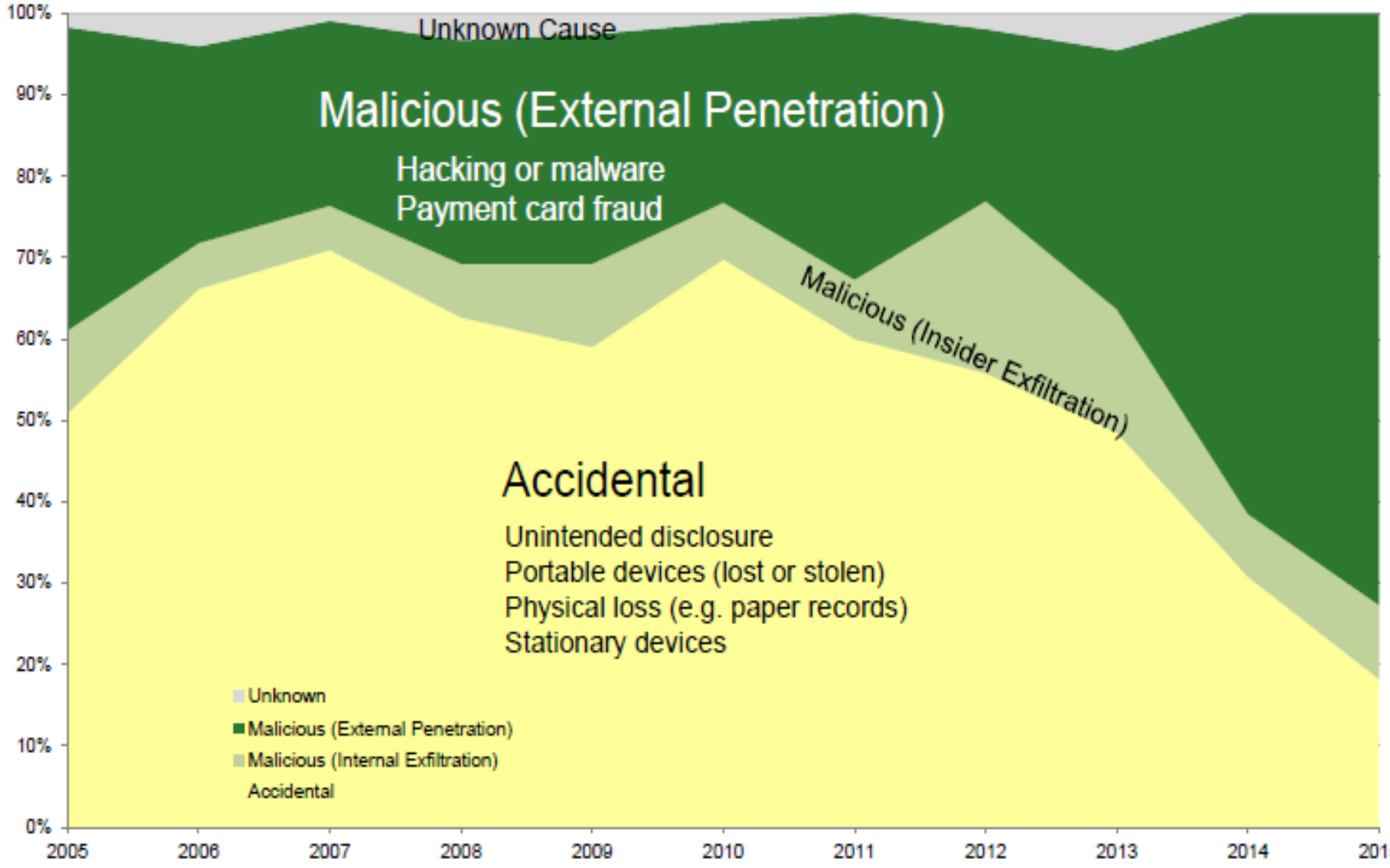
- 2000s Stand alone cyber offering mainly from global insurers
- 2013 Larger organizations (banks/retailers) purchasing cyber protection
- 2014 Insurers develop cyber offerings in 13 markets
  Changes to Australian Privacy Act and ACORN launched
- 2017 Parliament passing laws mandating cyber security breaches

Cyber Risk in APAC
Cyber (Re) Insurance in Japan

- Two segments of cyber like policies
  - Information Leakage Liability policy
  - Cyber policy
- 5 carriers provide coverage in Japan Market
- Limited coverage in relation to “apology” expenses

4. Industry Research and Model

Causes of Data Exfiltration – Trends over Time



Source: RMS: Managing Cyber Insurance Accumulation Risk

Aggregation modelling–Knowledge
Major vendors: Aggregation models

As at: Q2 2017	Lloyd's	RMS	AIR	Symantec
Model	• Cyber-attack Scenarios	• Cyber Accumulation Management System	• Analytics of Risk from Cyber	• CyberCube
Cyber Security Partner	• Various	• Cambridge Centre for Risk Studies • BitSight • Security Scorecard	• BitSight • Risk Based Security	• Symantec
Release Date	• v1 Q3 2016	• v1 Q3 2016 • v2 Q1 2017 • v3 Expected June 2018	• v1 Q2 2017 • v2 Expected in 2018	• v1 Q1 2018
Coverages	• Data Breach, BI, Silent	• Data Breach, BI, Silent	• Data Breach, BI, Silent	• Data Breach, BI
Scenario Catalogue	• 1 IT RDS • 2 IT scenarios • 5 OT scenarios	• 5 IT scenarios in v1 • 5 OT scenarios in v2 • Includes Lloyd's-like scenarios	• 4 IT scenarios in v1 • Supports own scenarios • Includes Lloyd's-like scenarios	• 23 IT scenarios in v1 • Includes Lloyd's-like scenarios
Scenario Narratives	• Public	• Public	• Public	• Proprietary
Scenario Parameters	• Public	• Proprietary	• Proprietary	• Proprietary
Probabilistic	• No	• No	• No	• Yes
Minimum Input	• n/a	• Industry (Occupancy), Size, Country, Policy Terms	• Industry (Occupancy), Size, Country, Policy Terms	• Industry (Occupancy), Size, Country, Policy Terms
Summary Output	• Scenario Impacts	• Exposure profiles and Scenario Impacts	• Exposure profiles and Scenario Impacts	• Exposure profiles and Year Loss Tables

Source: GC Research Q2 2017

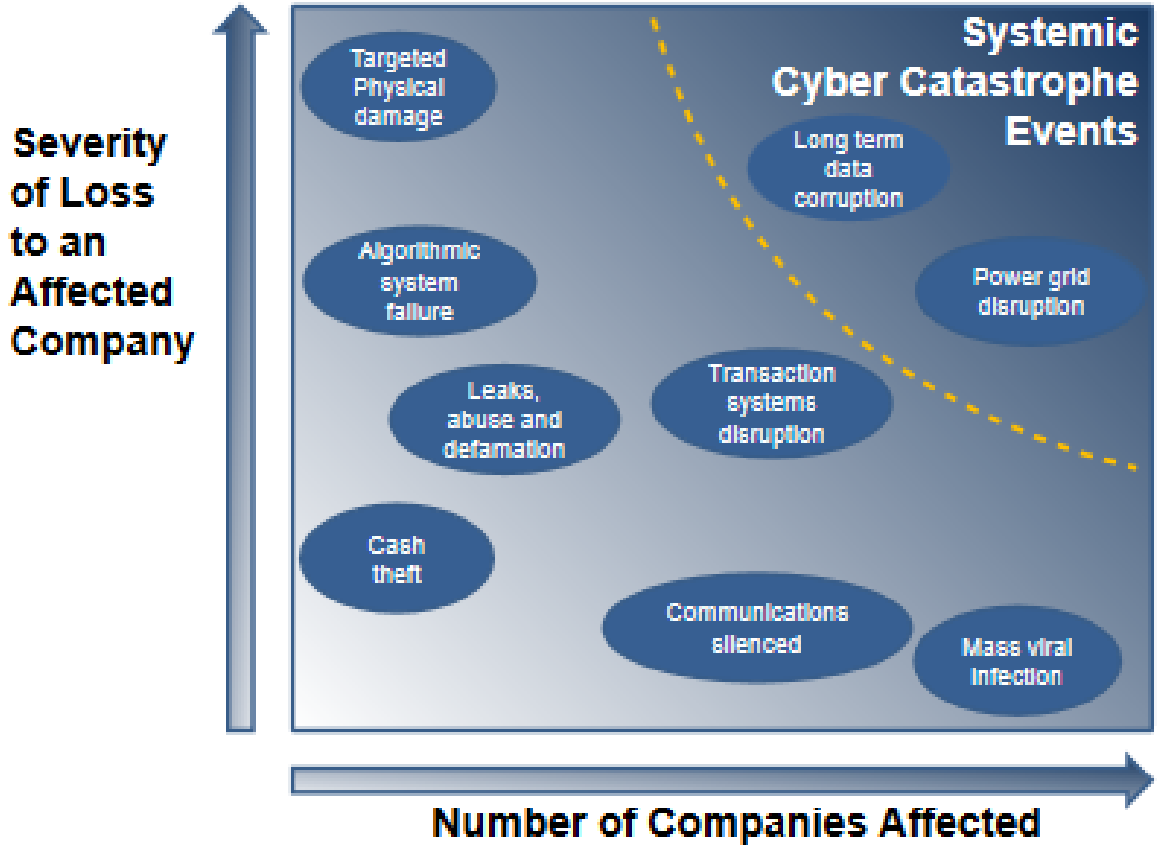
Aggregation modelling–Knowledge
Major vendors: Scenario coverage

As at: Q2 2017	Lloyd's	RMS	AIR	Symantec
Data Breach	✓	✓	✓	✓
US Blackout *	✓	✓	✓	✓
UK Blackout *	✓	✓	✓	✓
Cloud Provider Failure	✓	✓	✓	✓
Cyber Extortion		✓		✓
Denial of Service		✓	✓	✓
Financial Theft		✓		✓
Offshore Energy *	✓	✓		
Aviation *	✓			
Marine *	✓	✓		
Industrial Plant Fire *		✓		
Commercial Office Fire *		✓		

** OT Scenarios*

Source: GC Research Q2 2017

Industry Research and Model
Systemic Cyber Catastrophe Events



Source: by Lloyd's and the University of Cambridge's Centre for Risk Studies

Industry Research and Model
Deterministic Scenario - Business Blackout

Business Blackout

A hypothetical scenario of an electricity blackout that plunges 15 US states including New York City and Washington DC into darkness and leaves 93 million people without power.

- A piece of malware infects electricity generation control rooms
- 50 generators overload and burn out
- Parts of the region remain without electricity for **a number of weeks**

Economic impacts include direct damage to assets and infrastructure, decline in sales revenue to electricity supply companies, loss of sales revenue to business and disruption to the supply chain.

- The total economic loss is estimated at $243bn, rising to more than $1trn in the most extreme version of the scenario
- The total insurance loss is estimated at $21.4bn, rising to $71.1bn in the most extreme version of the scenario

Source: by Lloyd's and the University of Cambridge's Centre for Risk Studies

Industry Research and Model
Deterministic Scenario - Business Blackout

Insurance Industry Loss Estimation

CLASS	LINE OF BUSINESS	
Property		
	Personal Lines/Homeowner	0
	Personal Contents	2
	Commercial Combined	5
	Construction & Engineering	1
	Commercial Facultative	4
	Binding Authorities	0
Casualty		
	Workers' Compensation	1
	Directors & Officers	3
	Errors & Omissions	3
	Financial Lines	3
	General Liability	4
	Healthcare Liability	0
	Professional Lines	1
	Professional Liability	2
Auto		
	Personal Lines	-1
	Commercial & Fleet	-2

CLASS	LINE OF BUSINESS	
Life & Health		
	Life Insurance	0
	Health Insurance	2
	Income Protection	2
	Death & Disability	0
	Hospital Cover	-3
Pension and Annuities		
	Standard Annuities	0
	Variable Annuities	0
	Enhanced Annuities	0
	Life Settlements	0
War & Political Risk		
	Kidnap & Ransom	0
	Political Risk	2
	Political Violence & Terrorism	1
	Product Recall	3
	Trade Credit	4
Agriculture		
	Multi-peril Crop	0

Marine & Specie		
	Cargo	0
	Marine Hull	0
	Marine Liability	1
	Specie	1
Aerospace		
	Airline	2
	Airport	3
	Aviation Products	1
	General Aviation	1
	Space	0
Energy		
	Downstream	5
	Energy Liability	5
	Onshore Energy & Power	0
	Upstream	0
Specialty		
	Accident & Health	1
	Aquaculture Insurance	0
	Contingency – Film & Event	4
	Equine Insurance	2
	Excess & Surplus	1
	Surety	0

	Crop Hail	0
	Livestock	0
	Forestry	0
	Agriculture	1
Cyber Cover		
	Standard Data Breaches	1
	Advanced Property	5

KEY TO CHANGE IN INSURANCE CLAIMS	
Major decrease in claims	-5
	-4
	-3
	-2
	-1
No change in claims	0
	1
	2
	3
	4
Major increase in claims	5

Source: by Lloyd's and the University of Cambridge's Centre for Risk Studies

Industry Research and Model
Deterministic Scenario - Sybil Logic Bomb Cyber Catastrophe

Logic Bomb

An imaginary world leading database vendor, Sybil, has 50% market share. A logic bomb corruption is placed into a routine upgrade of the Sybil database software product. A long latency period (15 to 24 months) between activation and discovery of the logic bomb is crucial to the catastrophic nature of the scenario.

GICS Industry Group	Fictional Company	Fictional Failure	Real life precedents	Loss Mechanisms
Automobiles and Components	UK Auto Group	In UK Auto Group, an automobile manufacturing facility, a 9-foot robotic swings around 180 degrees despite the controller for the arm being in standby mode. 3 workers are killed. The SCADA system controlling the facility was being fed operating parameters from a compromised Sybil database.	"Ping Sweep": Robotic arm out of control (Duggan, Berg, Dillinger, & Stamp, 2005) [21]	Workers' compensation.
Banks	Albion Bank	For two years at UK based Albion Bank they failed to notice an error in interest rate calculations caused by erroneous data from their compromised Sybil database. They are forced to write off $1.75 billion. Company directors are sued by the shareholders for loss of share value.	National Australia Bank, 2001:HomeSide write-downs, $2.2Bn loss. (The Cost of Bad Data, 2013) [22]	Loss of assets; Loss in market value; Directors and Officers liability
Insurance	Eviva	A UK insurance company, Eviva, admits it has lost all record of thousands of customer policies. A system based on a Sybil Database that is used to scan and archive paper documents in bulk is discovered to be altering numbers randomly	Xerox WorkCentre Document Scanning Flaw (Kriesel, 2013) [23]	Loss of digital assets, loss in customer confidence, recovery costs

Source: by University of Cambridge's Centre for Risk Studies

Industry Research and Model
Deterministic Scenario – CAT Modelling Vendors

CAT Modelling Vendors

The risk modeling firms AIR Worldwide and RMS have developed cyber exposure databases for a large number of companies that can be used to build a detailed picture of possible losses under various deterministic scenarios.

What Are Examples of Cyber Scenarios That Can Be Modeled Deterministically?

CYBER DATA THEFT	Data breaches have been the most publicized incidents to date. The types of data that are at risk include names, emails, passwords, health or financial records, and intellectual property. Hackers have been known to use a variety of techniques to steal this data—social engineering, phishing, deploying malicious internal agents, and others—all of which can be modeled with the Verisk Cyber Exposure Data Standard.
VULNERABLE OR UNSUPPORTED SOFTWARE	Hackers are constantly looking for holes within popular software products to exploit. These "zero day" vulnerabilities do not get addressed by vendors when a product reaches its end-of-life point. Despite this risk, many people continue to rely on unsupported products. For example, about 12% of computers around the world still use Windows XP, which is no longer supported by Microsoft. If a new flaw is discovered, it will not be patched, leading to a potential aggregation loss.
ACCIDENTAL CYBER DATA LOSS	The more people an organization employs, the more likely it is that one of them makes a mistake and exposes data. Typically, this scenario consists of mobile devices such as laptop computers, USB drivers, or even a briefcase containing printouts of sensitive information being lost or misplaced. By assigning a probability of an employee losing data, insurers can estimate the associated losses.
DENIAL-OF-SERVICE (DOS) ATTACK	Many hackers are motivated by pride or politics. Their goals are more visibly served by shutting down their victims and those victims' operations than by stealing their data or money. One tactic that these types of hackers use is the denial-of-service (DoS) attack. DoS attacks work by overwhelming a target's network with a massive number of requests, effectively denying legitimate users from accessing the target's services. When lost revenue, incident response costs, or reputational damage occurs, the target can make a cyber insurance claim.
CLOUD SERVICE PROVIDER FAILURE	Companies of all industries and sizes have been outsourcing significant portions of their operations to cloud service providers, but the efficiency benefits gained from this shift do come with a risk. The top five cloud service providers own over half the market. If any of these providers were to experience downtime or a breach, their customers would suffer losses. With the Verisk Cyber Exposure Data Standard, insurers can perform aggregation analyses for their books of business and model the impact of contingent business interruption (CBI) or data record loss resulting from a cloud service provider failure.

Source: AIR Cyber Risk Solutions

CyberCube
Cyber Catastrophe Scenario Probability Models

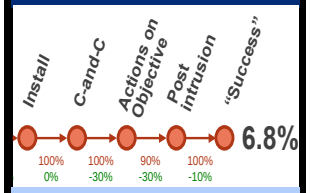
Scenario catalogue *12 scenario generation techniques resulting in 100s of potential scenarios*
~100 priority scenarios covering the material risks impacting insurers, with ~23 deeply modeled

1. Scenario probability

Data from the world's largest cyber security company

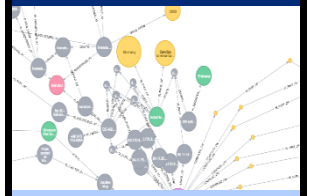
World's largest civilian Intelligence network across 6 threat centers

Kill Chain



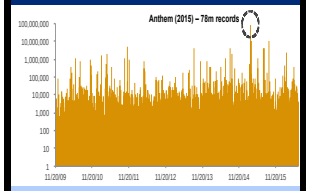
Probabilistic Kill Chain Framework

Threat Modeling



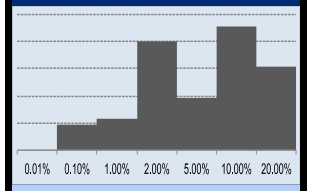
Threat Intelligence

Historical Model



Historical Data

Expert Model



Expert Surveys

>700 aggregation events, theoretical attacks and near misses

130 person expert panel

How often will cyber catastrophe events happen?

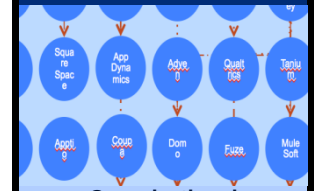
2. Footprint

1,200 specific single points of failure

Interconnections

Virtual / physical value chains

Firmographics



Organizational statistics

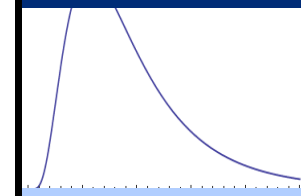
>7MM company data set

Which organizations are affected?

3. Financial impact

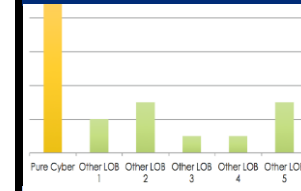
>50K publicly disclosed cyber events with actual or modeled losses for >20K

Cost modeling



Actuarial modeling

Cyber / Silent



Multi-LOB framework

CyberCube modeling, calibrated with partners

What are the financial losses for organizations and insurers?

Industry Research and Model
Probabilistic Model - GC ForCas ® CYBER

Overview

- Experience-based approach leveraging database of economic cyber losses
- Factors considered in determining frequency and severity distributions:
  - Industry Sector
  - Parent Type (Government, Non Profit, Private, Public, etc.)
  - Size of Company (Parent Revenue with Employee Count as proxy)
- Frequency incorporates historical industry-level correlations
- Produces ground-up loss distributions for insurer's cyber insurance portfolio
- Affirmative cover readily modeled, silent cover/endorsements can be included with proper premium allocation

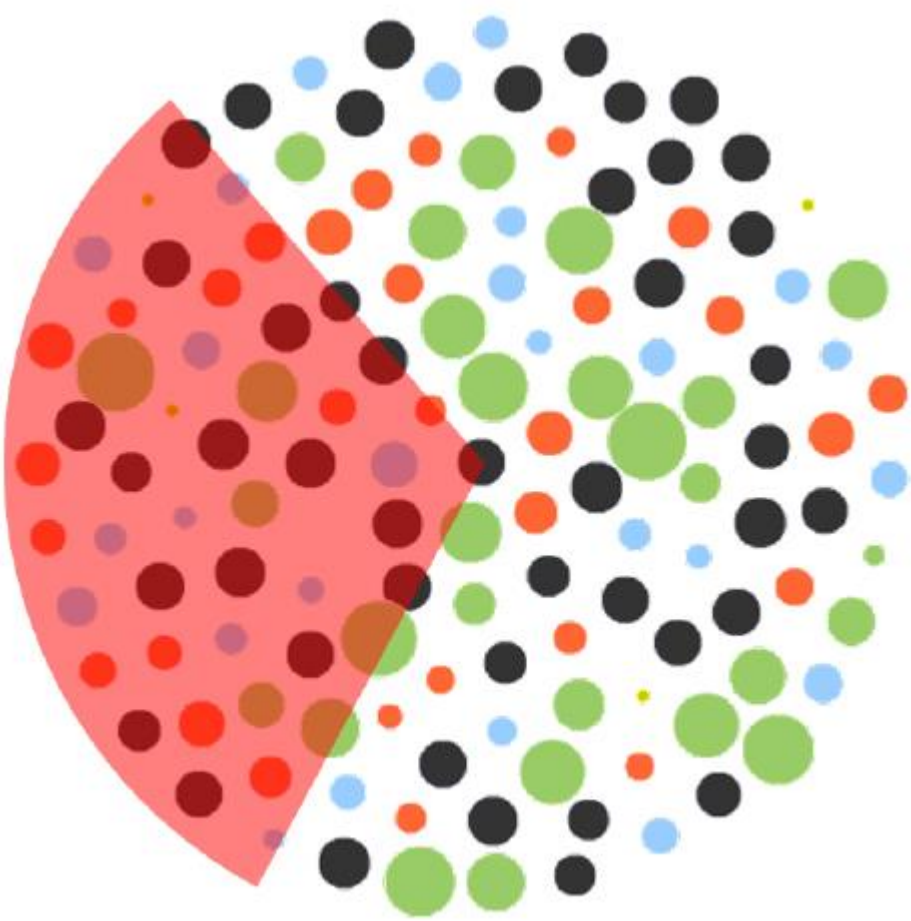
5. Model Data Input and Output

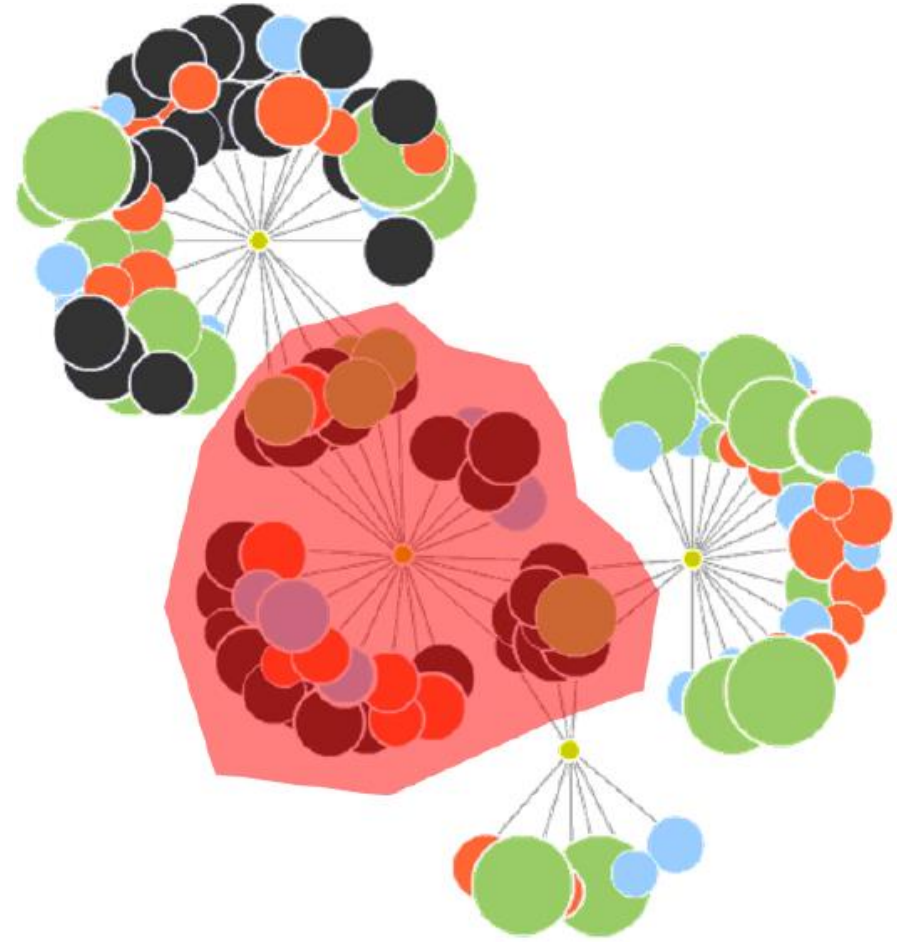
CyberCube
Model Input

CyberCube Model Input

- Insured Name
- Industry (Occupancy)
- Company Size
- Country
- Policy Terms

Model Input
Why Accurate Insured Name is Important?



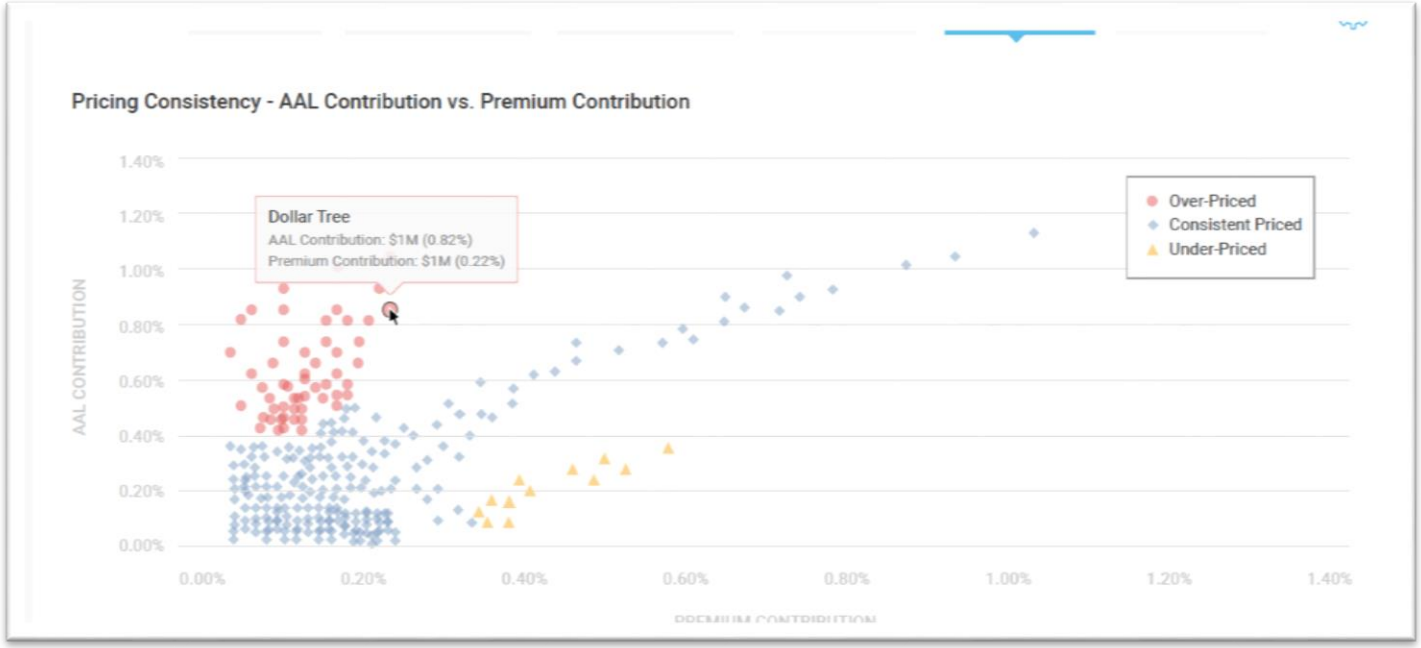


Source: AIR Cyber Risk Solutions

CyberCube
Model Output

CyberCube Model Output

- Loss AAL, OEP and AEP
- Year Loss Table
- Loss Summary by Scenario
- UW Performance Evaluation



6. Underwriting Coverage

Underwriting Coverage
Wide Variation in Cyber Coverage

v1.0 Code	Cyber Loss Coverage – Primary Category	Lloyd's Min Recommended	1st party	3rd party	Description
1	**Breach of privacy event**	Security Breach of Privacy	1st		The cost of responding to an event involving the release of information that causes a privacy breach, including notification, compensation, credit-watch services and other third party liabilities to affected data subjects, IT forensics, external services, and internal response costs, legal costs.
2	**Data and software loss**	Replacement of Lost Data and Software	1st		The cost of reconstituting data or software that have been deleted or corrupted.
3	**Network service failure liabilities**	Security Breach of Privacy		3rd	Third-party liabilities arising from security events occurring within the organisation's IT network or passing through it in order to attack a third-party.
4	**Business Interruption**	Business Interruption	1st		Lost profits or extra expenses incurred due to the unavailability of IT systems or data as a results of cyber attacks or other non-malicious IT failures.
5	**Contingent Business Interruption**	Business Interruption		3rd	Business interruption resulting from the IT failure of a third party, such as a supplier, critical vendor, utility, or external IT services provider.
6	**Incident response costs**	Security Breach of Privacy	1st		Direct costs incurred to investigate and close the incident to minimise post-incident losses. Applies to all the other categories/events.
7	**Regulatory and defence coverage**	Regulatory Fines	1st		Covers the legal, technical or forensic services necessary to assist the policyholder in responding to governmental inquiries relating to a cyber attack, and provides coverage for fines, penalties, defence costs, investigations or other regulatory actions where in violation of privacy law, and other costs of compliance with regulators and industry associations. Insurance recoveries are provided where it is permissible to do so.
8	**Liability – Product and Operations**	Liability		3rd	Third party liabilities arising in relation to product liability and defective operations.
9	**Liability – Technology Errors & Omissions**	Tech E&O / Programming ENO		3rd	Coverage for third party claims relating to failure to provide adequate technical service or technical products including legal costs and expenses of allegations resulting from a cyber attack or IT failure.
10	**Liability – Professional Services Errors & Omissions**	Liability		3rd	Coverage for third party claims relating to failure to provide adequate professional services or products (excluding technical services and products) including legal costs and expenses of allegations resulting from a cyber attack or IT failure.

Source: RMS: Managing Cyber Insurance Accumulation Risk

Underwriting Coverage
Wide Variation in Cyber Coverage

11	**Liability – Directors & Officers**	Liability	1st		Costs of compensation claims made against the individual officers of the business, including for breach of trust or breach of duty resulting from cyber-related incidents and can result from alleged misconduct, or failure to act in the best interests of the company, its employees, and its shareholders.
12	**Multi-media liabilities (defamation and disparagement)**	Liability	1st	3rd	Cost for investigation, defence cost and civil damages arising from defamation, libel, slander, copyright / trademark infringement, negligence in publication of any content in electronic or print media, as well as infringement of the intellectual property of a third party.
13	**Financial theft & fraud**	Extortion	1st		The direct financial loss suffered by an organisation arising from the use of computers to commit fraud or theft of money, securities, or other property.
14	**Reputational damage**	Reputational Damage / Public Relations	1st		Loss of revenues arising from an increase in customer churn or reduced transaction volumes, which can be directly attributed to the publication of a defined security breach event.
15	**Cyber extortion**	Extortion	1st		The cost of expert handling for an extortion incident, combined with the amount of the ransom payment.
16	**Intellectual property (IP) theft**	Replacement of Lost Data and Software	1st		Loss of value of an IP asset, expressed in terms of loss of venue as a result of reduced market share.
17	**Environmental damage**	Physical Damage	1st		Cover for costs of clean up, recovery and liabilities associated with a cyber induced environmental spill or release.
18	**Physical asset damage**	Physical Damage	1st		First-party loss due to the destruction of physical property resulting from cyber attacks.
19	**Death and bodily injury**	Bodily Injury		3rd	Third-party liability for death and bodily injuries resulting from cyber attacks.

Source: RMS: Managing Cyber Insurance Accumulation Risk

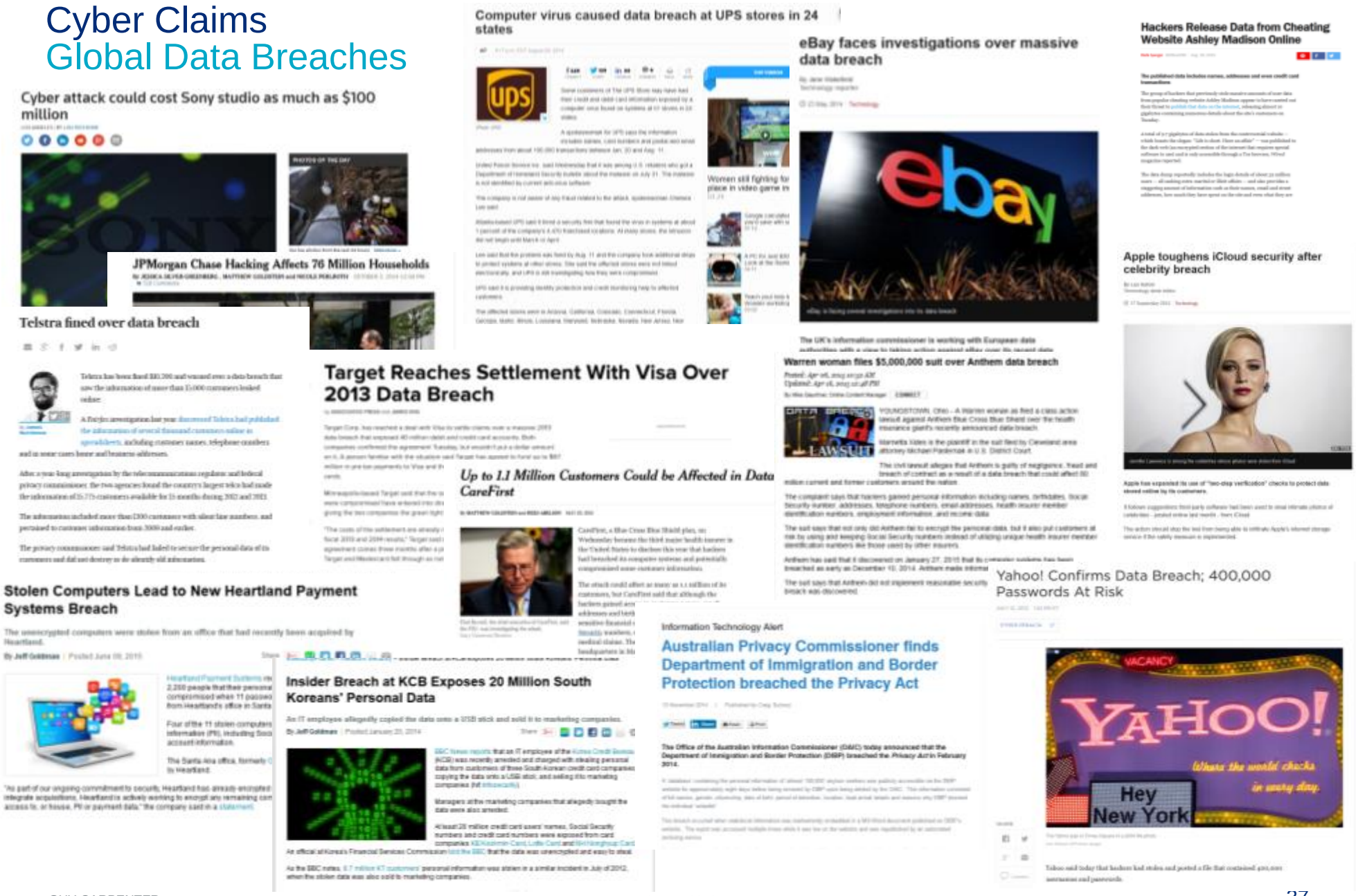
Underwriting Coverage
Wide Variation in Cyber Coverage

v1.0 Code	Cyber Coverage	% of Products Offering this Cover (Sample of 26)
1	Breach of privacy event	92%
2	Data and software loss	81%
6	Incident response costs	81%
15	Cyber extortion	73%
4	Business interruption	69%
12	Multi-media liabilities (defamation and disparagement)	65%
7	Regulatory and defense coverage	62%
14	Reputational damage	46%
3	Network service failure liabilities	42%
5	Contingent Business Interruption	33%
9	Liability – Technology Errors & Omissions	27%
10	Liability – Professional Services Errors & Omissions	23%
13	Financial theft & fraud	23%
16	Intellectual property (IP) theft	23%
18	Physical asset damage	19%
19	Death and bodily injury	15%
-	Cyber terrorism	12%
11	Liability – Directors & Officers	13%
8	Liability – Product and Operations	8%
17	Environmental damage	4%

Source: RMS: Managing Cyber Insurance Accumulation Risk

7. Cyber Claims

Cyber Claims
Global Data Breaches



Cyber Claims
Target Breach

A cyber attack started on November 27, 2013, Target personnel discovered the breach and notified the U.S. Justice Department by December 13th.

40 million credit and debit cards and **70 million** non-card customer information are stolen by hackers during that 3 weeks period.

The starting point of that cyber attack is compromising a third-party vendor.

Path:
Vendor-portal access → Gain control of Target servers → Point of sale (POS) systems

Cyber Claims
Target Breach

As of January 2017, Target has incurred $292 million in breach-related costs including legal fees, crisis communications and forensics costs.

- $67 million settlement with Visa
- $19 million settlement with MasterCard
- $20 million settlement with Discover and American Express
- $10 million settlement with customers

At the time of the breach, Target had $100 million in cyber insurance coverage from multiple underwriters, on top of a $10 million deductible.

Cyber Claims
Other US Significant Breaches

Between April and September of 2014, malware planted on Home Depot's POS system compromised up to **56 million** credit and debit cards. As of January 2017, this breach has incurred **$298 million** in expenses, which will be partially offset by **$100 million** in insurance proceeds.

In February 2015, **78.8 million** personally identifiable information were stolen from Anthem, the largest for-profit managed health care company in the Blue Cross and Blue Shield Association. As of December 2015, the hack has already cost Anthem about **$230m** in legal and consultant fees.

Yahoo! reported two major data breaches of user account data to hackers during the second half of 2016. The first announced breach, reported in September 2016, had occurred sometime in late 2014, and affected over **500 million** Yahoo! user accounts. A separate data breach, occurring earlier around August 2013, was reported in December 2016, and affected over **1 billion** user accounts.

Q&A

Keep Calm and Ask An Actuary