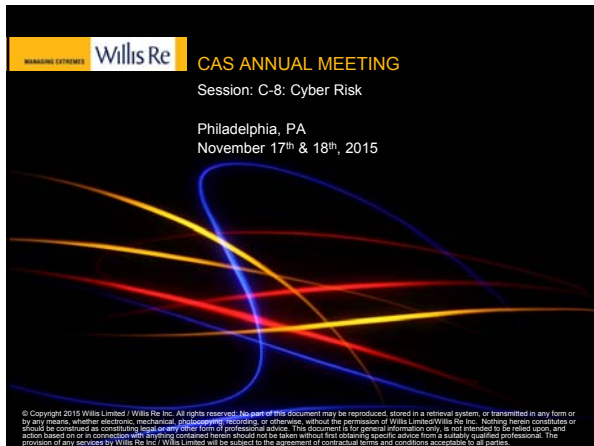
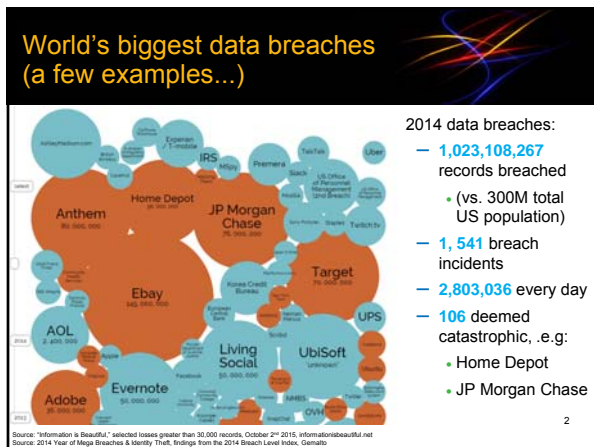


WILLIS TOWERS WATSON
Willis Re CAS ANNUAL MEETING
 Session: C-8: Cyber Risk
 Philadelphia, PA
 November 17th & 18th, 2015



© Copyright 2015 Willis Limited / Willis Re Inc. All rights reserved. No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without the permission of Willis Limited/Willis Re Inc. Nothing herein constitutes or should be construed as constituting legal advice or professional services. This document is for general information only. It is intended to be read, copied, and action based on or in connection with anything contained herein should not be taken without first obtaining specific advice from a suitably qualified professional. The provision of any services by Willis Re Inc. / Willis Limited will be subject to the agreement of contractual terms and conditions applicable to all practices.

World's biggest data breaches (a few examples...)

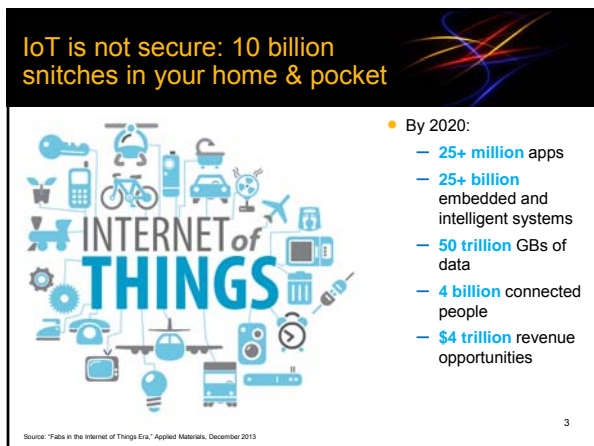


2014 data breaches:

- 1,023,108,267 records breached
 - (vs. 300M total US population)
- 1,541 breach incidents
- 2,803,036 every day
- 106 deemed catastrophic, .e.g:
 - Home Depot
 - JP Morgan Chase

Source: "Information is Beautiful," selected losses greater than 50,000 records, October 2nd 2015, informationisbeautiful.net
 Source: 2014 Year of Mega Breaches & Identity Theft, findings from the 2014 Breach Level Index, Gemalto

IoT is not secure: 10 billion snitches in your home & pocket

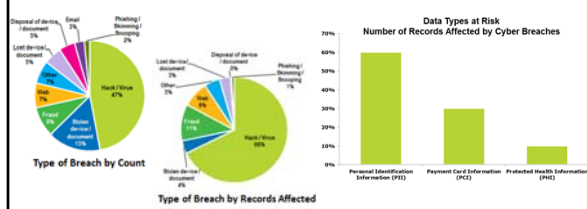


By 2020:

- 25+ million apps
- 25+ billion embedded and intelligent systems
- 50 trillion GBs of data
- 4 billion connected people
- \$4 trillion revenue opportunities

Source: "Fads in the Internet of Things Era," Applied Materials, December 2013

Major causes and costs of data breach

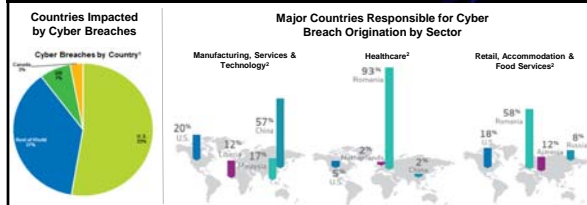


- Less than half of all breaches are caused by hacking / malware attacks, but these breaches are generally larger in size
- Number of PII records affected is almost twice the number of PCI records affected

All charts are based on the RBS database, September 2014.

4

Historical breaches: observations by region



- U.S. breaches comprise more than 50% of available data
 - Likely due to mandatory privacy breach disclosure laws in U.S.
- U.S. not the main region of breach origination
- Region of breach origination differs by sector

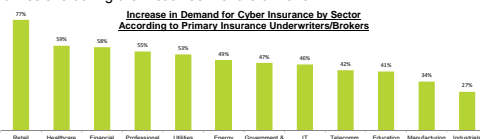
¹ Based on the RBS database, September 2014.

² Verizon Threat Landscape Research Reports on Retail, Accommodation & Food Services and Financial Services Sectors, 2013.

5

Growing demand for cyber insurance

- Headline news about cyber attacks and data breaches give rise to increased demand for cyber insurance
- A **\$2.4 billion industry in US today**, projected to growth significantly over next 5-10 years
 - PWC estimates worldwide premium \geq \$7.5B by 2020
 - Allianz projects \$20 billion by 2025
- The London cyber insurance market has seen a **50% YOY rise** in insurance submissions during the first three months of 2015

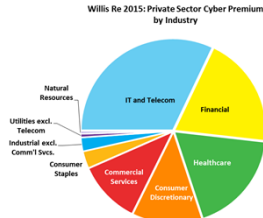


Source: Ashden Loss Insight: Headlines from the Cyber Risk Network, May 21, 2015.
 Source: "Cyber Risk the Most Serious Threat to Business, says Lloyd's Chief," The Telegraph, May 7 2015.
 Source: Ashden Cyber Liability Insurance market Trends Survey, October 2014.

6

Who are the buyers?

Purchasing is dominated by companies in IT & Telecom, Financial, and Healthcare



7

Analytics in the cyber space

Growth in the cyber industry forces (re)insurers to develop ways for quantifying cyber exposure

INSURERS

Vary in approach. Many insurers writing cyber have models for assessing individual insureds based on industry type, size, number of records and/or qualitative assessments of the insured's risk management procedures and risk culture

BROKERS

AON	MARSH	WILLIS
Cyber Risk Diagnostic Tool "provides a high level understanding of the cyber risks facing an organization"	Cyber IDEAL model "models probabilities and potential financial impacts of cyber events on individual organizations"	PRISM model for individual cyber risks and PRISM-Re model for insurer's cyber portfolio analysis; frequency / severity approach, full probabilistic models

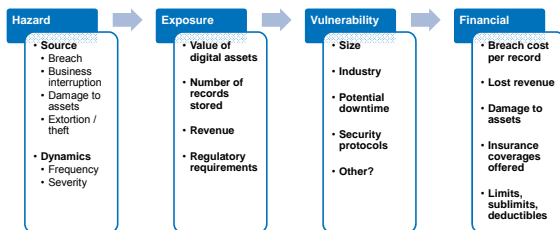
CAT MODELING FIRMS

AIR	RMS
Stochastic modeling framework in development phase; working prototype	Working on data schema; "eye to developing a model that can start gauging probabilities of attacks as early as next year"

8

*Risk modelers look to clarify cyber risk costs. Reuters, December 19th 2014.

Cyber risk underwriting should consider...



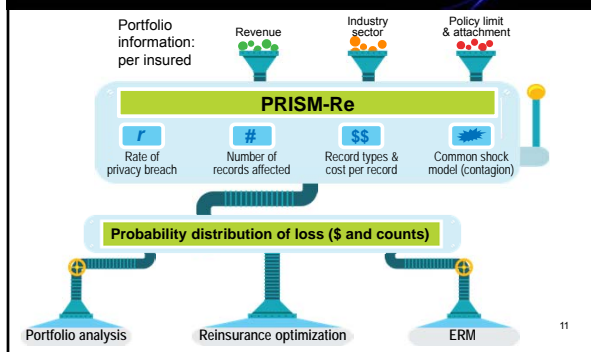
9

PRISM-Re™

- Willis Re's new proprietary **portfolio model for cyber risk**
 - Developed out of Willis PRISM™
 - Incorporates industry-leading expertise of the Willis Cyber Team
- Estimates a portfolio's exposure to **privacy breach**
 - Objective analysis of exposures using **current risk indicators**
 - Reflects **potential loss "contagion"** within / between industry sectors
- Applications
 - Estimate **downside risk** due to privacy breach
 - Track **risk-adjusted pricing** relativity over time
 - Monitor **shifts in the risk profile**
 - Indicate potential improvements to **portfolio composition**
 - **Allocate capital** to portfolio based on riskiness

10

PRISM-Re framework



11

PRISM-Re mechanics

