

**Cyber Insurance and
Quantifying The Exposure**

Casualty Actuarial Society
CAS Spring Meeting – Colorado Springs
May 2015

Moderator

- Joe Palmer, Vice President - Commercial Lines Actuarial | ISO

Panelists

- Anne M. Mason, Underwriting Manager | Hartford Financial Products - E&O/Cyber
- Eduard Goodman, J.D., LL.M., CIPP-US/C, Chief Privacy Officer | IDT911
- Dr. Tomas P. Girnius, Principal Scientist, Research and Modeling | AIR Worldwide

2

Cyber Risk Insurance

Anne M. Mason
Underwriting Manager
Hartford Financial Products
E&O / Cyber

What is Cyber Liability?

“Cyber Liability” and “Cyber Risk” means different things to different people.*

- Information Security – (52%)
- Network Security – (19%)
- Privacy – (13%)
- Data Breach – (11%)
- Network Breach – (5%)

“Cyber Liability” encompasses first- and third-party risks associated with networks, e-business, the Internet and possession of informational assets or “data”.

The risks include:

- Data Privacy
- Network Security
- e-Media or Internet Liability

4 Source: The Breakey Report See policy for actual coverage wording – general presentation use only

Data Breach - Statutes and Standards

• What are the laws and regulations?

- 47 State Breach Notification Laws and D.C. and Puerto Rico
- Calif. SB 1386, Mass. 93H-1, Nev. 603A.010: Very broad scope
- States with no security breach law: AL, NM, & SD
- 35 Federal Laws regarding privacy
- HIPAA, HITECH, GLB, FACTA, FERPA, COPPA
- Compliance Standards
- PCI, SAS 70 audit disclosures, Sarbanes-Oxley Section 404

• What is considered PII (personally identifiable information) and PHI (protected health information)?

- | | |
|--------------------------------|-----------------------------|
| - Individual names | - Health records |
| - Social Security numbers | - Financial account numbers |
| - Credit or debit card numbers | - Insurance plan ID numbers |
| - Drivers License numbers | - IP Address |
| - State ID numbers | - Login name, screen name |
| - Telephone numbers | - Zip codes |
| - Passport numbers | - Email addresses |
| - Dates of birth | |

5 See policy for actual coverage wording – general presentation use only

What Does Cyber Liability Insurance Cover?

Typical Insuring Agreements and Coverages:

- Data Privacy and Network Security Liability
 - Third party liability arising out of wrongful acts – violation of data privacy laws, improper collection or disclosure of PII; unauthorized access or unauthorized use of Insured’s computer system.
- Digital Media Liability
 - Online media liability - website or social media page
 - Copyright/trademark infringement, defamation, invasion of privacy
- Expense Coverages

- Breach Notification	- Regulatory Proceeding
- Credit Monitoring / Identity Protection	- PCI Fines
- Crisis Management	- Data Restoration
- Investigation	
- Cyber Business Interruption
- Cyber Extortion
- Professional Liability

6 See policy for actual coverage wording – general presentation use only

Cyber Liability Underwriting Factors?

- How large is the company?
- What is the customer base?
- What type of data is stored or shared?
- How many sensitive records?
- Is company compliant with applicable data privacy laws?
- Is sensitive data encrypted and where?
- Is there a formal privacy policy?
- Who is responsible for network security & data protection?
- Do vendor contracts address data privacy and security?
- Is there a Document Destruction/Management Plan?
- Is there a Data Breach Incident Response Plan?
- Is there a Business Continuity Response Plan?
- Aggregation issues – common vendors, cloud providers

7

This policy is actual coverage wording – general presentation use only

Cyber Liability Coverage...what's trending?

- Business Interruption
- Dependent Business Interruption
- Electronic Data Restoration expenses
- Full limits for expense coverages
- Privacy notification benefits expanded
 - Costs for computer expert services
 - Legal services for breach notifications
 - Call center services
 - Payment Card Industry fines & penalties
 - Courtesy/voluntary notifications and credit monitoring
- eFunds coverage / Funds Transfer Fraud
- E-commerce extortion
- Cyber Terrorism

8

This policy is actual coverage wording – general presentation use only

CYBER RISK INSURANCE: Quantifying the Exposure


Eduard Goodman, J.D., LL.M., CIPP-US/C/E
Chief Privacy Officer



© 2014 IDT, LLC. All Rights Reserved. Confidential



01 Agenda

Today's objectives: 

- **Define** what a Data Breach is
- **Clarify** the real data exposures scenarios that lead to data breaches (and how to prevent them)
- **Recognize** the value in pre and post breach management approaches to handling these complex claims

May 1, 2015 © IDT911, LLC. All Rights Reserved. Confidential 11

02 What is a data breach?

IDT911

What is a data breach? (Generally)

A data breach is any exposure of private or confidential information held by an entity (business, government entity, etc.). This exposure could be through loss, theft or other method of exposure. This data can include:

- Confidential Company Data such as:
 - Business plans
 - Client lists
- Private Personal information such as:
 - Personally Identifiable Information
 - Protected Health Information
 - Account Information

May 1, 2015 © IDT911, LLC. All Rights Reserved. Confidential 11

IDT911

What is a data breach? (Private Personal)

YOUR PII CHART™

LEGEND

- SOCIAL SECURITY NUMBER**
SSN (not SSAN)
- CONTACT INFORMATION**
Home & business, cellular & wireless, e-mail, fax, mobile, pager & landline
- GOVERNMENT-ASSIGNED IDENTIFICATION**
Driver's License, passport, birth certificate, Birth card
- BIRTH DATE, BIRTH PLACE**
- ONLINE INFORMATION**
Blogs, social media, accounts, IP#
- SECUCATION**
Institutions, GPA, transcript
- VERIFICATION DATA**
Brokers, professions, post office box, phone, fax, email & password
- MEDICAL RECORDS INFORMATION**
Prescriptions, medical records, x-rays, images
- ACCOUNT NUMBERS**
Bank, insurance, investments, credit cards


May 1, 2015 © IDT911, LLC. All Rights Reserved. Confidential 11

IDT911

What is a data breach? (Legally Speaking)

Under state breach notification laws, businesses must notify consumers if there has been a breach that exposes their unencrypted Personally Identifiable Information (PII).

May 1, 2015 © IDT911, LLC. All Rights Reserved. Confidential 11

Personally Identifiable Information 

Typically Name and Address with:


- Social Security Number
- Account Numbers
 - Sometimes only if PIN or other access info is released
- Driver's license numbers
- State issued ID numbers

May 1, 2015 © 2015 ILL. All Rights Reserved. Confidential 19

Data Breach Incidents (Estimated)
from 1/1/2005 through 4/27/15 

4517
Breaches made public (min)

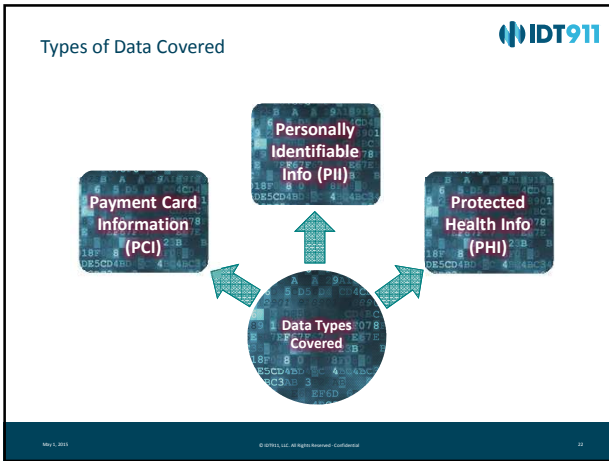
816,324,756
Records containing personal/private info of U.S. citizens and residents

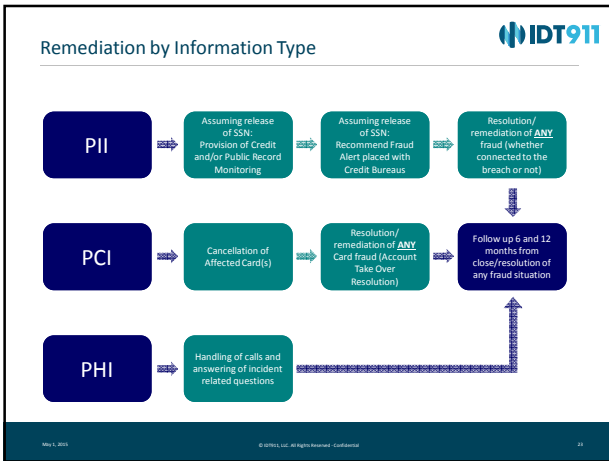


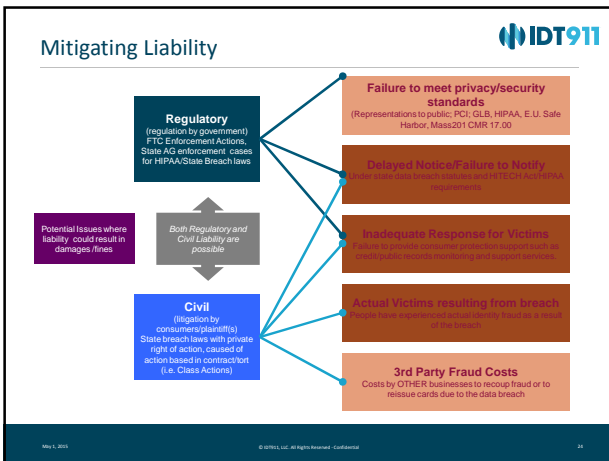
Source: <http://www.privacyrights.org/data-breach/new>

May 1, 2015 © 2015 ILL. All Rights Reserved. Confidential 20

03 Liability and Remediation by Breach Type







Anderson v. Hannaford Brothers

Potential Damages by affected consumers of breach

ACTUAL VICTIM LOSSES
(Unreimbursed Fraudulent Charges)
COMPENSABLE

deemed recoverable damages

Actual victims of fraud who suffer permanent financial losses as a direct result of the breach. For example:

- Card breaches where amounts removed as a result of the data exposure are **unreimbursed** by the bank or financial institution. (This rarely happens)
- Where SSN's are exposed by a breach, then affected consumers with IDT (new account creation) that cannot be resolved by end of litigation. (Often difficult to connect to the breach)

MITIGATION COSTS
(Under Hannaford)
rarely **COMPENSABLE**

POTENTIAL recoverable damages

NEW POTENTIAL DAMAGES THEORY - Reasonable fees expended by the consumer to mitigate the potential damages to accounts and identity. For example:

- Cost of replacement card fees when the issuing bank declined to issue a replacement card to them
- Damages for the purchase of identity theft/card protection insurance
- Damages for the purchase of credit monitoring services

NON-MITIGATION COSTS
NON-COMPENSABLE

NOT deemed recoverable damages

- Fees for accounts overdrawn by fraudulent charges
- Fees for altering pre-authorized payment arrangements
- Loss of accumulated reward points
- Inability to earn reward points during the transition to a new card
- Emotional distress related to fear or apprehension of becoming a victim
- Time and effort spent reversing unauthorized charges and protecting against further fraud

May 1, 2013 © IDT911 LLC. All Rights Reserved. Confidential 25

Empirical Analysis of Data Breach Litigation

Temple University Beasley School of Law
LEGAL STUDIES RESEARCH PAPER NO. 2012-29

Electronic copy available at: <http://ssrn.com/abstract=1986461>

May 1, 2013 © IDT911 LLC. All Rights Reserved. Confidential 26


Two Key Questions

Which data breaches are being litigated in federal court?

Which data breach lawsuits settle?

May 1, 2013 © IDT911 LLC. All Rights Reserved. Confidential 27

Liability in Terms of Odds-Ratios



The odds of a firm being sued are...


- 3.5X** greater when individuals suffer actual (financial) harm
- 6X** lower when the firm provides free credit monitoring to those affected by the breach

The odds of a firm being sued from improperly disposing data are...

- 3X** greater than breaches caused by lost/stolen data
- 6X** greater when the data breach involved loss of financial information

May 1, 2013 © IDT911, LLC. All Rights Reserved. Confidential 28

Probability of Data Breach Settlement



Probability of Settlement

- 30% Increase** Plaintiff allegations of financial harm
- 30% Increase** The certification of a case as a "class action"

Surprisingly, causes of action asserting a violation of a federal statute with statutory damages were not positively correlated with settlement.

May 1, 2013 © IDT911, LLC. All Rights Reserved. Confidential 29

04 The '9' Data Breach Scenarios

Missing or Stolen Laptop/Storage Device IDT911

Situation: Policyholder reports a missing computer device storing Personally Identifiable Information (PII), such as a laptop, USB flash drive or portable hard drive

Possible Scenarios

- Laptop stolen from a parked vehicle at the mall
- Luggage containing a laptop or portable storage device fails to arrive at destination
- Laptop or portable storage device stolen from a place of business or a home office

April 01, 2013
Doctor's stolen laptop found at pawn shop, data of 652 patients exposed

January 17, 2013
'Terrific Employee' Fired After Losing USB Drive Containing Medical Records

May 1, 2013 © IDT911, LLC. All Rights Reserved. Confidential 11

Mis-mailing IDT911

Situation: Policyholder reports that documents with one person's PII were mistakenly sent to someone else

Possible Scenarios

- Documents faxed to the wrong number
- Bill, statement of benefits, or other documents sent to wrong person or address
- Attachments containing PII emailed to incorrect recipient

March 26, 2013
Texas Tech University Health Sciences Center Admits Data Breach
Approximately 700 patient billing statements were mistakenly sent to other patients' mailing addresses.

January 25, 2013
Officials At Cheyney U. Warning Students About Personal Data Breach
An administrative email sent to all students included a file with personal data.

May 1, 2013 © IDT911, LLC. All Rights Reserved. Confidential 12

Erroneous Data Posting IDT911

Situation: Policyholder posts or prints PII in a public venue

Possible Scenarios

- Erroneous web site posting
- Failure to redact PII that may become public record prior to submission to a government entity

April 05, 2013
Medical records of 2k patents left unprotected on contractor's server

12/19/2012
California Accidentally Posts 14,000 Social Security Numbers

May 1, 2013 © IDT911, LLC. All Rights Reserved. Confidential 13

IDT911

Breach Caused by a Third Party Vendor

Situation: Policyholder utilizes an outside vendor for services that involve PII or PHI of the Policyholder's customers, clients or employees and the vendor had a breach

Possible Scenarios

- Payroll processor or benefits provider suffers a breach that exposes employee PII
- Business process vendors lose data while handling PII for Policyholders

May 1, 2013 © IDT911, LLC. All Rights Reserved. Confidential 17

IDT911

Improper Document/Equipment Disposal

Situation: Policyholder improperly disposes of documents or equipment that contain PII or PHI of the Policyholder's customers, clients or employees

Possible Scenarios

- Backup data tape submitted for destruction is unaccounted for
- Documents and/or document destruction storage areas are left unsecured
- Documents/equipment containing PII are improperly disposed of or are recycled or left exposed

May 1, 2013 © IDT911, LLC. All Rights Reserved. Confidential 18

IDT911


Insider

Situation: Policyholder reports that an employee or contractor accessed files containing PII for reasons unrelated to their job function

Possible Scenarios

- A disgruntled employee announced his resignation and then was caught copying files from his computer to a flash drive
- A curious employee accessed his co-workers HR files

May 1, 2013 © IDT911, LLC. All Rights Reserved. Confidential 19



QUESTIONS?

Eduard Goodman, J.D., LL.M., CIPP-US/C/E
Chief Privacy Officer
Scottsdale, Arizona
480.355.4940 direct
EGoodman@IDT911.com

May 1, 2015 © 2015 IDT LLC. All Rights Reserved. Confidential 11

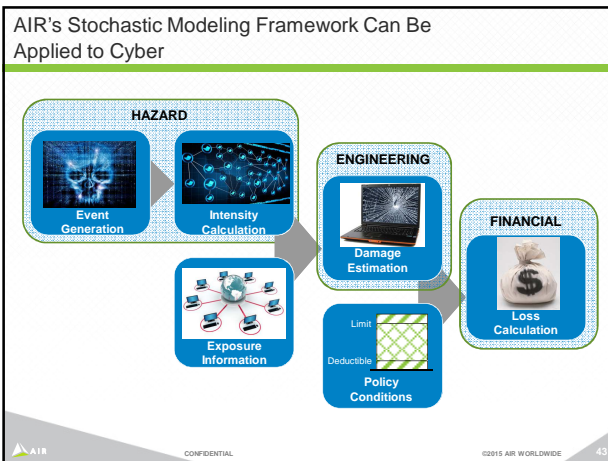
**New Approaches for
Managing Cyber Risk**



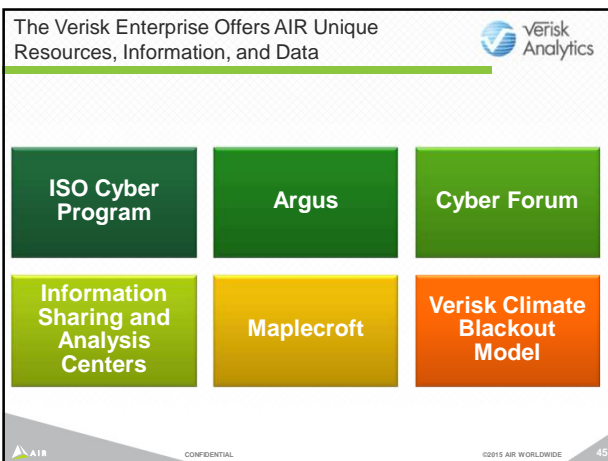
Agenda

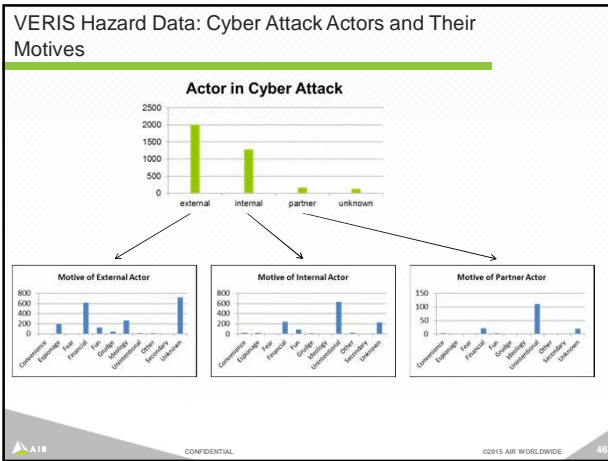
- AIR modeling framework
- Potential data partners
- AIR cyber data standards
- Roadmap

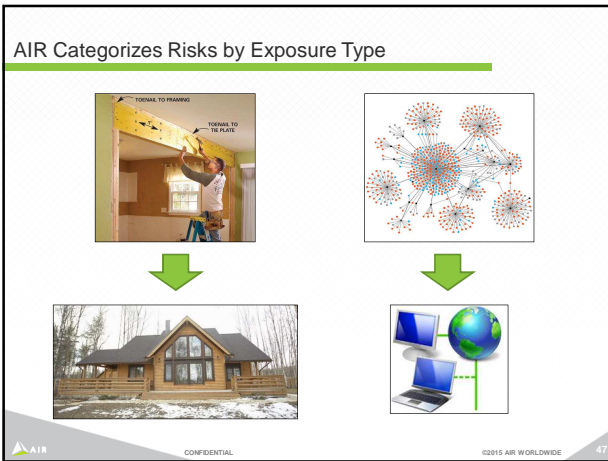
AIR CONFIDENTIAL © 2015 AIR WORLDWIDE 42

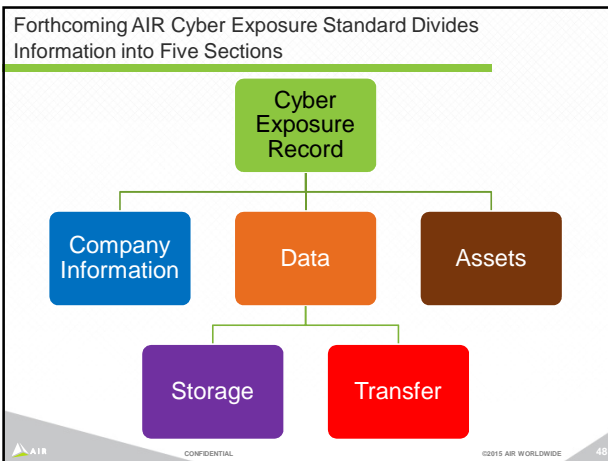


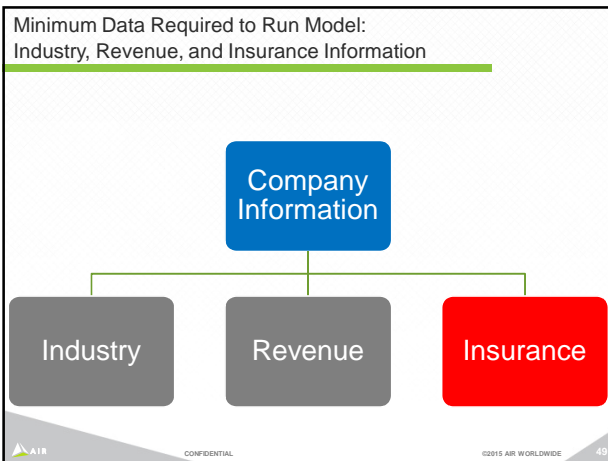




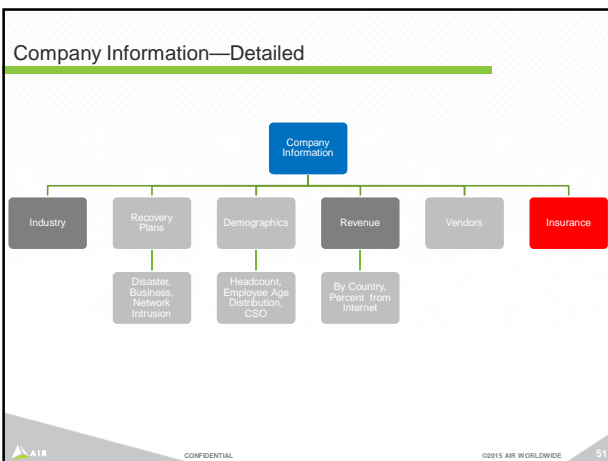


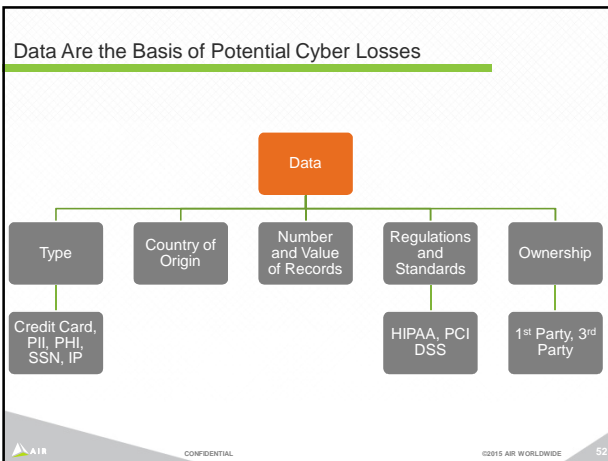


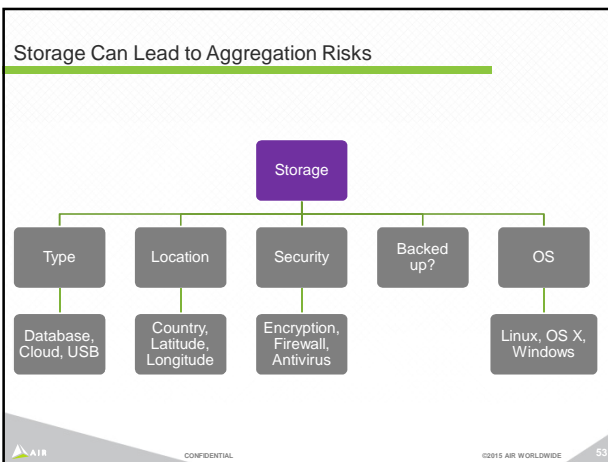


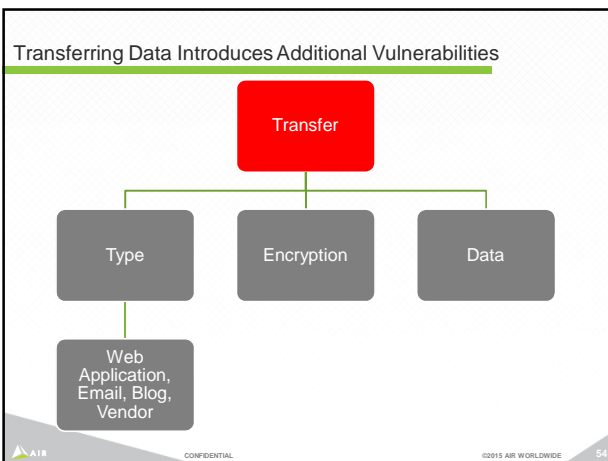


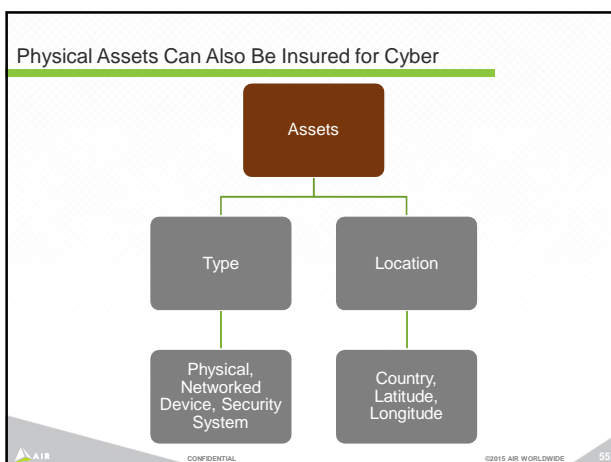
- Multiple Insurance Coverages May be Supported
- Insurance Coverages**
- Security Breach Expense
 - Security Breach Liability
 - Business Interruption
-
- Fines
 - Replacement of Electronic Data
 - Web Site Publishing Liability
 - Programming Errors and Omissions
 - Extortion
 - Public Relations
 - Physical
- AIR CONFIDENTIAL ©2015 AIR WORLDWIDE 50











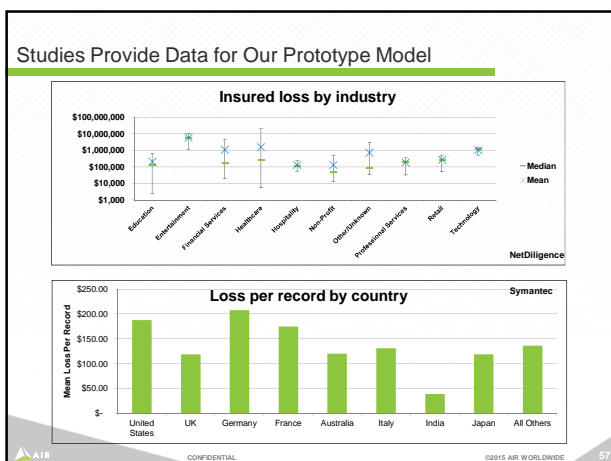
Developing a Cyber IED Will Allow the Model to Account for "Unknowns"

- Most refined results are obtained when every field of an exposure record is correctly filled in
- But what if we have only some of the information that completely describes an exposure?
- AIR's Cyber Model will populate "unknown" fields with values derived from our planned Cyber Industry Exposure Database

Data	Type	Record Value	Country of Origin	Ownership
	Credit Card	\$225	U.S.	3 rd Party
	PII	\$99	U.S.	1 st Party

Annual Revenue	Total	% from Internet	% Domestic	% Foreign
	1,300,000,000	17%	72%	28%

©2015 AIR WORLDWIDE 56



The "Hurricane Andrew" of Cyber Is Coming



AIR CONFIDENTIAL ©2015 AIR WORLDWIDE 58

Aggregation Is More than the Cloud



AIR CONFIDENTIAL ©2015 AIR WORLDWIDE 59

AIR's Prototype Cyber Framework and Its Roadmap

Catalog	Frequency of attack data from sample VERIS breach database	Stochastically generated breach events	In talks to get a much more comprehensive dataset	
Exposure	Over 400 companies in our sample exposure database	Getting Internet footprint data, to help build a cyber ICD	Data standards in Touchstone 4.0	
Vulnerability	10 key basic risk factors, including company industry and encryption	Potential to add third party "scores" as secondary features	Soliciting feedback on whether our characteristic list is "missing" a critical feature	
Loss	Loss per record information from Synscan, accounting for risk features	Framework calibrated to the reported loss from the 2013 Target breach	Partnering with insurance companies to receive cyber loss data	Modeling of aggregation of losses
Model	Results and reports available through consulting studies	Deterministic and probabilistic results	Will be in Touchstone in the future	

AIR CONFIDENTIAL ©2015 AIR WORLDWIDE 60
