IRUA February 6th Cyber Seminar

Libby Benet
Beazley Specialty Treaty Underwriting
February 6, 2017

beazley

Cyber liability and data breach

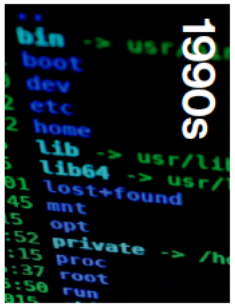
Stat of the market

What is the Exposure to Risk?

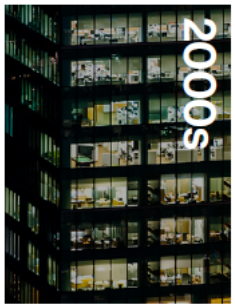
What are common coverages?

The timeline below explores how cyber risk has grown in just a few decades to become one of today's most pressing issues on the boardroom agenda.

The internet is a closed-off world, dominated by academics and hobbyists. Curious hackers develop a reputation for both good and bad behaviours becoming known as "white-hats" and "black-hats", respectively. "Hacking" has recreational and educational purposes but, inevitably, other motivations prevail and over time the internet loses some of its early innocence.



By the mid-1990s the internet starts to reach mainstream consumers who are often easy prey for criminal attacks. As more businesses come online, computerised systems are regularly attacked, sensitive and financial data becomes a criminal commodity and denial-of-service techniques become weaponised. By the late 1990s the first incident of cyber espionage is reported.



The internet is now a regular part of life for most people and an accepted field of business and government activity. More sophisticated cyber threats emerge, such as financial Trojan malware (see section 2.3) and the hijacking of millions of online banking sessions, coupled with a dramatic increase in the number of data breaches. The rise of smartphones makes mobile the new frontier of cyber risks. This decade also sees the first allegations of military cyberattacks, in Estonia (2007) and Georgia (2008).

The battle between cyber criminals and cyber security firms reaches maturity, each developing their own tools and reverse-engineering each other's to gain an advantage. While cyber security is a $75 billion marketplace[3], front-line cybercriminals thrive in a black market where high-end exploitation tools can reportedly change hands for up to a million dollars. Cybercrime costs business an estimated $400 billion annually, and mirrors the legitimate growth of the digital economy, now estimated to be worth $4.2 trillion[4]. The internet of things is likely to become the new cyber battleground.

Cyber Insurance: Size of the Market and Market Players

Two good places to look for information on the market:

The Betterley Report, by Richard S. Betterley, www.betterley.com; and

The NAIC Cyber Supplement

NAIC Cyber Supplement

- Regulators at the state and federal level are concerned about the exposure. They think insurers can help insureds risk manage the exposure.
- Began in 2015 so we have 2 years of data.
- They are looking to understand 3 segments:
    - Stand alone cyber and Cyber as endorsement to a package
    - Personal lines ID Theft products
- According to the NAIC, the initial filings were received April 1, 2016 for 2015 data and the second year of filings were received in April 2017 for 2016 data.
- Analysis for 2016 data showed more than 500 insurers provided business and individuals with cyber insurance in the U.S.
- The vast majority of these coverages were written as endorsements to commercial and personal policies.
- NAIC estimates the cyber market is $2.49B.

NAIC Cyber Supplement 2016

- For the admitted market: premium for standalone policies was $920,712,006 and package policies was $434,475,892. The total written premium for both types of policies was $1,784,481,175

2016 Report	
$920,712,006	Standalone
$434,475,892	Package
$429,293,277	Unreported estimate
$1,784,481,175	Estimated Market Size

- For the surplus lines market: premiums for standalone policies was $552,226,000 and package policies was $156,285,000. The total written premium for both types of policies was $708,511,000.

2016 Report	
$552,226,000	Standalone
$156,285,000	Package
$708,511,000	Market Size

- 98% of the liability coverage is written on a claims made basis.

*http://www.naic.org/documents/cmte_ex_cybersecurity_tf_rpt_cyber_ins_coverage_suppliment.pdf?786

The Cyber Market – Stand Alone Policies*

- 42 insurer groups (128 individual insurers)
- Insurers writing this coverage reported $920,712,006 in direct written premium
- The top ten insurers wrote 68.7% of total U.S. market with the top 20 writing 84.4% of the market
- The standalone cybersecurity insurance written premium for 2016 has increased by 90.5% since last year.
- Loss ratios for standalone cybersecurity insurance were all over the map ranging from zero to over 400%.

*http://www.naic.org/documents/cmte_ex_cybersecurity_tf_rpt_cyber_ins_coverage_suppliment.pdf?786

The Cyber Market - Top 10 Standalone Markets

- Hanover Insurance Group Inc.
- Tokio Marine Group
- Hartford Financial Services
- Travelers Companies Inc.
- NASW Risk Retention Group Inc.
- Beazley Insurance Co.
- Chubb Ltd.
- CNA Financial Corp.
- American International Group
- XL Group Ltd

This groups represents 83% of the stand alone market by policy count and 79% based on premium.

*Data is as reported in the NAIC Supplement for 2016.

The Cyber Market – Package Policies*

- 356 Companies reported premium.
- 352 insurers of the 708 insurers reported no premiums, generally because they could not break out the premium change for the cybersecurity coverage from the remainder of the package policy.

*http://www.naic.org/documents/cmte_ex_cybersecurity_tf_rpt_cyber_ins_coverage_suppliment.pdf?786

The Cyber Market – Top 10 Package Markets*

- Hartford Financial Services
- Farmers Insurance Group of Cos
- Erie Insurance Group
- Berkshire Hathaway Inc.
- Selective Insurance Group Inc.
- United Fire Group Inc.
- Brotherhood Mutual Ins Co.
- Hanover Insurance Group Inc.
- Travelers Companies Inc.
- CNA Financial Corp.

This groups represents 74% of the package market by policy count!

*Data is as reported in the NAIC Supplement for 2016.

The Cyber Market – Top 10 Package Markets*

- American International Group
- Chubb Ltd.
- AXIS Capital Holdings Ltd.
- CNA Financial Corp.
- Travelers Companies Inc.
- Berkshire Hathaway Inc.
- Farmers Insurance Group of Cos
- Beazley Insurance Co.
- Aspen Insurance Holdings Ltd.
- Fosun International Hldgs Ltd.

This groups represents 85% of the package market by premium!

*Data is as reported in the NAIC Supplement for 2016.

The Cyber Market – Personal Lines ID Theft

- According to the NAIC report there were 21.4 million policies including identity theft coverage as part of a package policy. This compares to only 278,334 policies that were stand-alone identity theft coverage.

2016 Report	
$23,800,000.00	Standalone
$502,900.00	Package
$24,302,900.00	Market Size

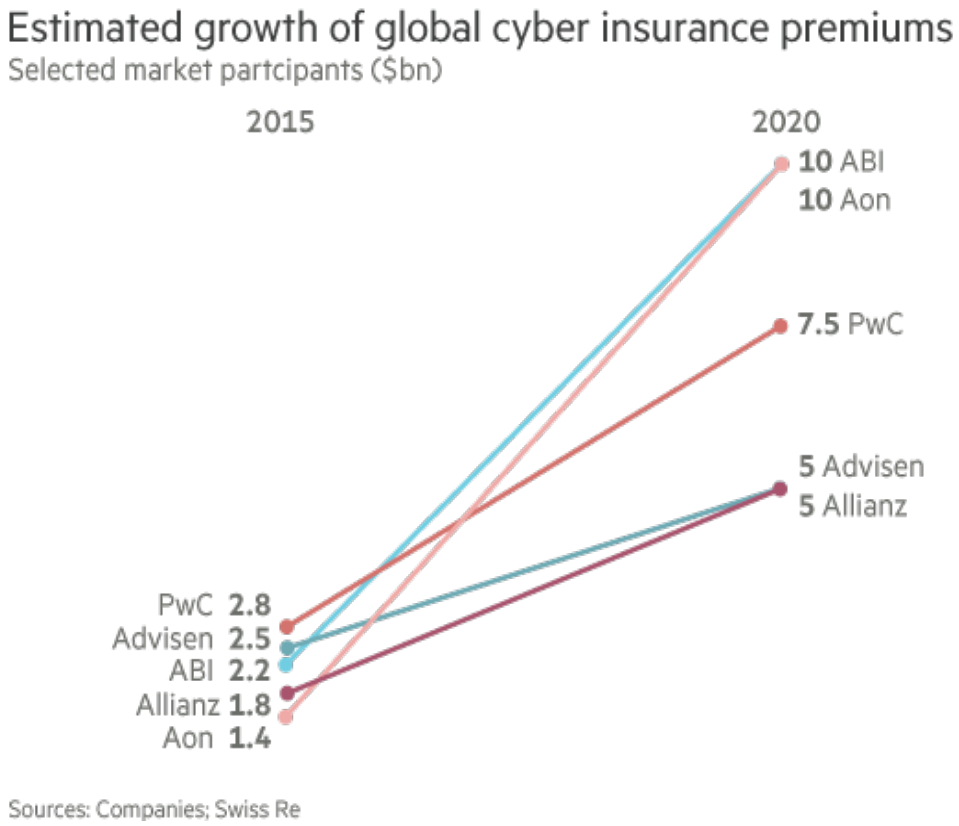
*http://www.naic.org/documents/cmte_ex_cybersecurity_tf_rpt_cyber_ins_coverage_suppliment.pdf?786

The Cyber Market – Top 10 Personal Lines

- Nationwide Mutual Group
- Chubb Ltd.
- State Farm Mutl Automobile Ins
- Travelers Companies Inc.
- Allstate Corp.
- Liberty Mutual
- Hanover Insurance Group Inc.
- Erie Insurance Group
- Farmers Insurance Group of Cos
- American Family Insurance Grp

This groups represents 77% of the personal lines market by premium!

The cyber and data breach market projections



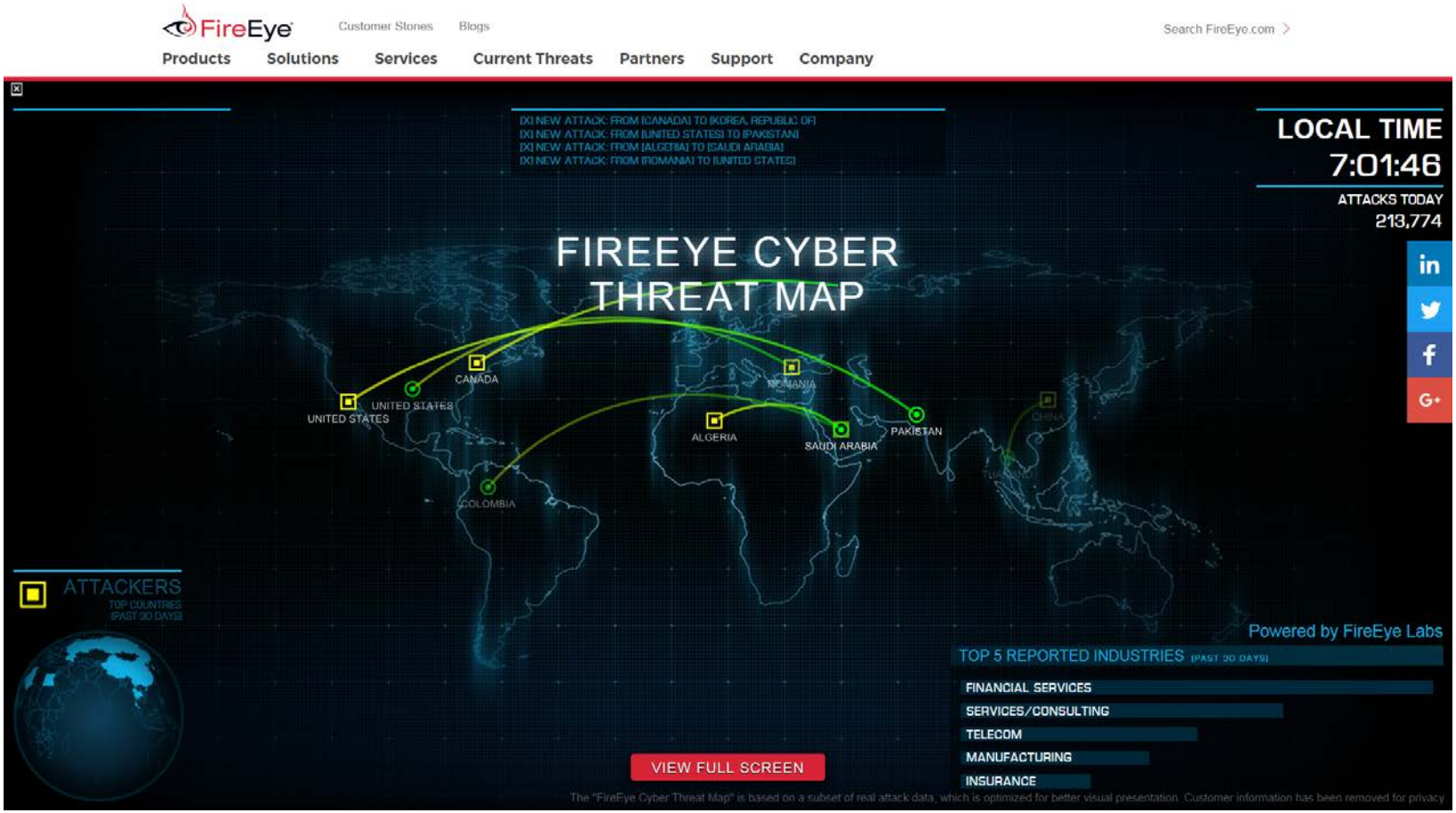
The market is still considered in its infancy in terms of penetration levels, estimated to be under 15% in the US

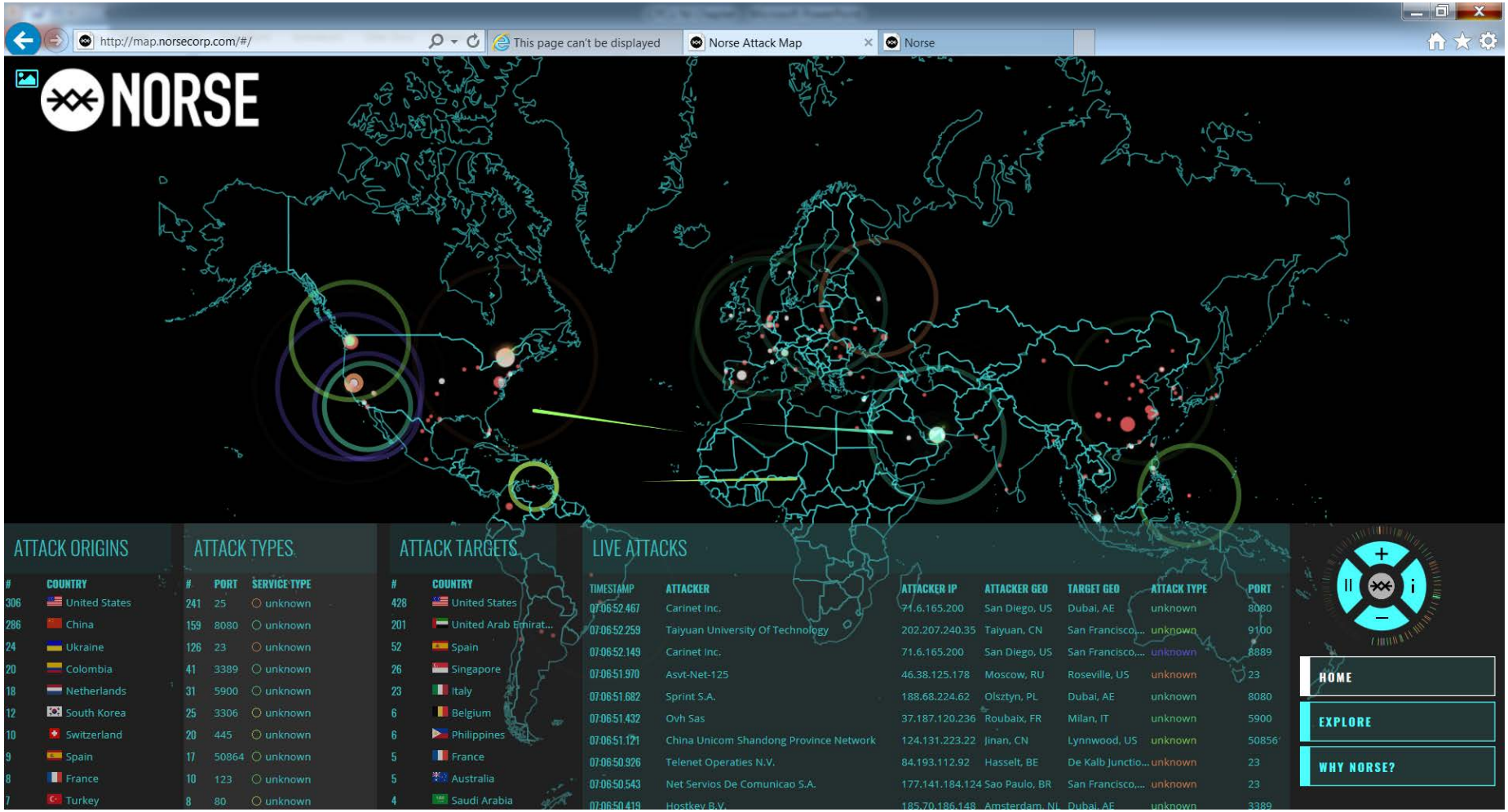
Cyber liability and data breach

State of the market

What is the Exposure to Risk?

What are common coverages?


FireEye
Customer Stories
Blogs
Search FireEye.com
Products
Solutions
Services
Current Threats
Partners
Support
Company
[X] NEW ATTACK: FROM [CANADA] TO [KOREA, REPUBLIC OF]
[X] NEW ATTACK: FROM [UNITED STATES] TO [PAKISTAN]
[X] NEW ATTACK: FROM [ALGERIA] TO [SAUDI ARABIA]
[X] NEW ATTACK: FROM [ROMANIA] TO [UNITED STATES]
LOCAL TIME
7:01:46
ATTACKS TODAY
213,774
FIREEYE CYBER THREAT MAP
CANADA
UNITED STATES
UNITED STATES
ROMANIA
ALGERIA
SAUDI ARABIA
PAKISTAN
CHINA
COLOMBIA
ATTACKERS
TOP COUNTRIES (PAST 30 DAYS)
Powered by FireEye Labs
TOP 5 REPORTED INDUSTRIES (PAST 30 DAYS)
FINANCIAL SERVICES
SERVICES/CONSULTING
TELECOM
MANUFACTURING
INSURANCE
VIEW FULL SCREEN
The "FireEye Cyber Threat Map" is based on a subset of real attack data, which is optimized for better visual presentation. Customer information has been removed for privacy.


http://map.norsecorp.com/#/
This page can't be displayed
Norse Attack Map
Norse
NORSE
ATTACK ORIGINS
COUNTRY
306 United States
286 China
24 Ukraine
20 Colombia
18 Netherlands
12 South Korea
10 Switzerland
9 Spain
8 France
7 Turkey
ATTACK TYPES
PORT SERVICE TYPE
241 25 unknown
159 8080 unknown
126 23 unknown
41 3389 unknown
31 5900 unknown
25 3306 unknown
20 445 unknown
17 50864 unknown
10 123 unknown
8 80 unknown
ATTACK TARGETS
COUNTRY
428 United States
201 United Arab Emirat...
52 Spain
26 Singapore
23 Italy
6 Belgium
6 Philippines
5 France
5 Australia
4 Saudi Arabia
LIVE ATTACKS
TIMESTAMP ATTACKER ATTACKER IP ATTACKER GEO TARGET GEO ATTACK TYPE PORT
07:06:52.467 Carinet Inc. 71.6.165.200 San Diego, US Dubai, AE unknown 8080
07:06:52.259 Taiyuan University Of Technology 202.207.240.35 Taiyuan, CN San Francisco,... unknown 9100
07:06:52.149 Carinet Inc. 71.6.165.200 San Diego, US San Francisco,... unknown 8889
07:06:51.970 Asvt-Net-125 46.38.125.178 Moscow, RU Roseville, US unknown 23
07:06:51.682 Sprint S.A. 188.68.224.62 Olsztyn, PL Dubai, AE unknown 8080
07:06:51.432 Ovh Sas 37.187.120.236 Roubaix, FR Milan, IT unknown 5900
07:06:51.121 China Unicom Shandong Province Network 124.131.223.22 Jinan, CN Lynnwood, US unknown 50856
07:06:50.926 Telenet Operaties N.V. 84.193.112.92 Hasselt, BE De Kalb Junctio... unknown 23
07:06:50.543 Net Servios De Comunicao S.A. 177.141.184.124 Sao Paulo, BR San Francisco,... unknown 23
07:06:50.419 Hostkey B.V. 185.70.186.148 Amsterdam, NL Dubai, AE unknown 3389
HOME
EXPLORE
WHY NORSE?

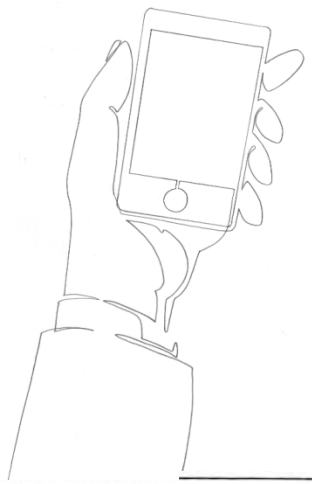
Where Are the Threats?

Inside threats

- Employee negligence
  - Security failures
  - Lost portable devices
  - Unintended disclosures by email, fax, phone or in person
- Failure to encrypt portable devices
- Employee ignorance
  - Improper disposal of personal information (dumpsters)
  - Lack of education and awareness
- Malicious and/or nosey employees

Outside threats

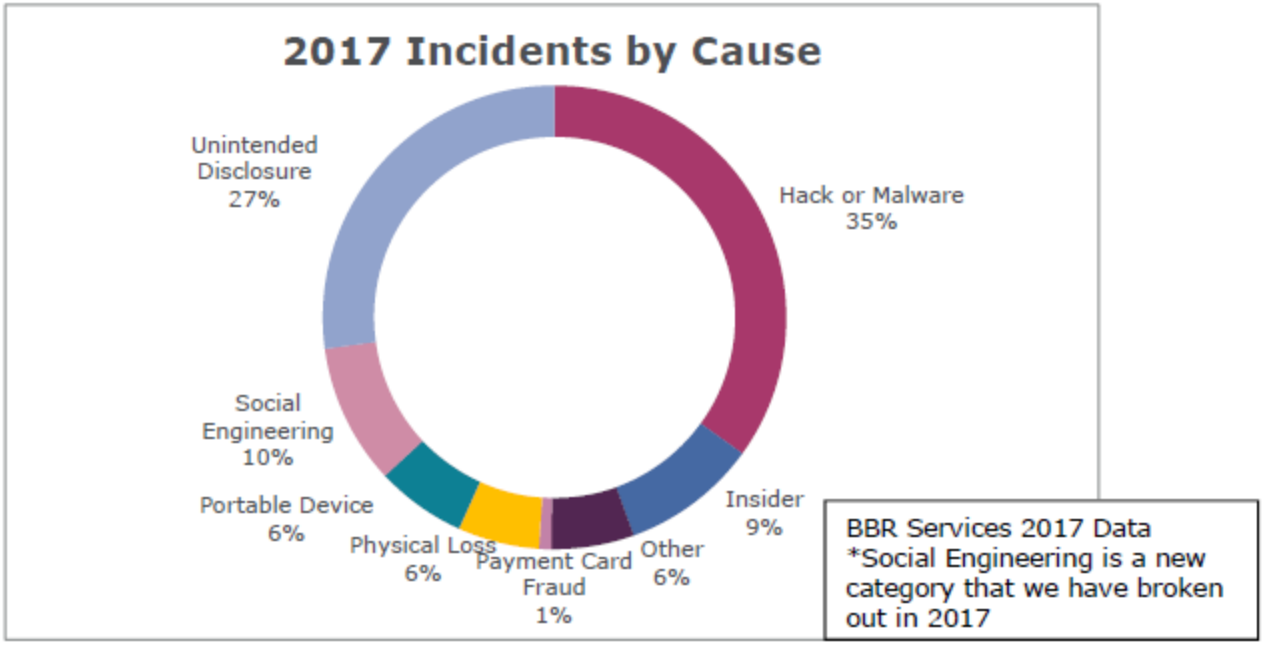
- Hackers
  - Malware
  - Phishing and spear phishing
- Thieves
  - Social engineering tools
  - Stolen portable devices
- Vendors/Business Associates



	Incidents				Breaches			
	Total	Small	Large	Unk	Total	Small	Large	Unk
Total	**42,068**	**606**	**22,273**	**19,189**	**1,935**	**433**	**278**	**1,224**
Accommodation (72)	215	131	17	67	201	128	12	61
Administrative (56)	42	6	5	31	27	3	3	21
Agriculture (11)	11	1	1	9	1	0	1	0
Construction (23)	6	3	1	2	2	1	0	1
Education (61)	455	37	41	377	73	15	15	43
Entertainment (71)	5,534	7	3	5,524	11	5	3	3
Finance (52)	998	58	97	843	471	39	30	402
Healthcare (62)	458	92	108	258	296	57	68	171
Information (51)	717	57	44	616	113	42	21	50
Management (55)	8	2	3	3	3	2	1	0
Manufacturing (31-33)	620	6	24	590	124	3	11	110
Mining (21)	6	1	1	4	3	0	1	2
Other Services (81)	69	22	5	42	50	14	5	31
Professional (54)	3,016	51	21	2,944	109	37	8	64
Public (92)	21,239	46	20,751	442	239	30	59	150
Real Estate (53)	13	2	0	11	11	2	0	9
Retail (44-45)	326	70	36	220	93	46	14	33
Trade (42)	20	4	10	6	10	3	6	1
Transportation (48-49)	63	5	11	47	14	3	4	7
Utilities (22)	32	2	5	25	16	1	1	14
Unknown	8,220	3	1,089	7,128	68	2	15	51
Total	**42,068**	**606**	**22,273**	**19,189**	**1,935**	**433**	**278**	**1,224**

Table 1: Number of security incidents by victim industry and organization size, 2016 dataset.

Claim Activity By Cause of Loss



Beazley 2017 Data

Different Industries Are Vulnerable to Different Cause of Loss

Industry	Unintended Disclosure	Hack or Malware	Social Engineering
Healthcare	39%	19%	3%
Financial	22%	48%	12%
Education	27%	43%	9%
Retail	4%	53%	30%
Professional Services	12%	48%	21%
Hospitality	4%	74%	9%

Beazley 2017 Data

The infographic is based on KPMG's analysis of publicly available references[9] and KPMG's industry insights.

Key

- Primarily targeted
- Frequently targeted
- Occasionally targeted
- Rarely targeted

The order of the circles in the same category does not indicate relative frequency.

9 CERT-UK, DoS A Rising Tide, 2016; Akamai, State of the Internet Report, Q1 2016; Verizon, Data Breach Report, 2016; Symantec, Ransomware and Businesses 2016, Ransomware Infections by Organization Sector, Jan 2015-Apr 2016; Bitsight Insights Report, The Rising Face of Cyber Crime: Ransomware, September 2016; Trend, Following the data, analysing breaches by industry, 2005-2015 data breach records; Ponemon, Cost of Data Breach Survey, 2015, Per capita cost by industry classification; Mandiant, M-TRENDS 2016

Breach Incidents – It Is Not All Cyber-Related

- Paper or Electronic
    - 12% of breach incidents involve paper
- Accidental or Intentional
    - 22% of breach incidents are broken business practices
- Company / 3rd Party
    - Approximately 30% of breach incidents are a result of a 3rd party

Source: Beazley – 2016 statistics

Where's the Risk? - Spectrum of Risk

Unintended Disclosure

- o Paper / Physical Records
  - Un-shredded Documents
  - Dumpster Diving
  - File cabinets – sold/donated
  - Natural Disasters
  - X-Ray Images

Where's the Risk? - Spectrum of Risk

Unintended Disclosure

- Electronic assets
  - Computers
  - Smart phones
  - Backup tapes
  - Hard drives
  - Servers
  - Copiers
  - Fax machines
  - Scanners
  - Printers

- Leasing Contracts - Review

Costs of breach consequences

- These questions will help you calculate business losses:
  - How much money will you lose based on information, such as intellectual property (IP) or personally identifiable information (PII), lost through the data breach?
  - How much money will you lose to notification costs, lawsuits, fines, audits and brand damage when the data breach becomes public?
  - How much time will it take to resolve the breach—to identify and address all affected systems, and respond to attacks?
  - How much will you be fined if your security practices don't comply with security policies and requirements?

Cost of a Data Breach at Market Rates				
Records	Privacy Counsel Fees	Forensics	Notification/Call Center	Total
100	$6,000-$12,000	$10,000-20,000	$500-$1,000	$16,500-$33,000
1,000	$15,000 - $30,000	$20,000-$32,000	$2,000-$6,000	$37,000-$76,000
10,000	$30,000-$40,000	$32,000-$80,000	$12,000-$40,000	$74,000-$360,000

Fire Eye https://www.fireeye.com/current-threats/cost-of-a-data-breach.html
And Beazley Claims Detail.

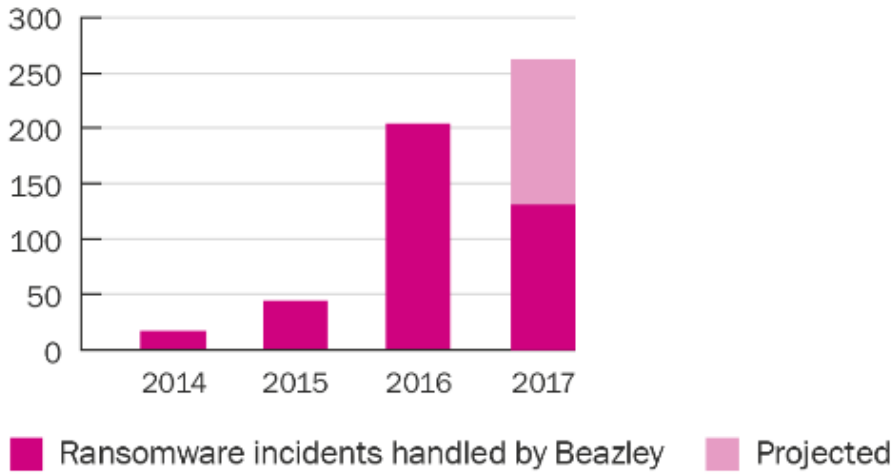
Ransomware – A Particular Kind of Computer Attack

- Ransomware is malware that typically enables cyber extortion for financial gain.
- Criminals can hide links to ransomware in seemingly normal emails or web pages.
- Once activated, ransomware prevents users from interacting with their files, applications or systems until a ransom is paid, typically in the form of an anonymous currency such as Bitcoin.
- Ransomware is a serious and growing cyber threat that often affects individuals and has recently made headlines for broader attacks on businesses.
- Payment demands vary based on targeted organizations, and can range from hundreds to millions of dollars.
- A multitude of ransomware variants exist.
    - They include Cryptolocker and its variants such as Kriptovor and Teslacrypt, Cerber, Dridex and Locky and most recently, WannaCry.

Fire Eye https://www.fireeye.com/current-threats/what-is-cyber-security/ransomware.html

Growing threats – cyber extortion

Ransomware incidents handled by Beazley



Beazley Breach Insights, August 2017

WannaCry, May 2017

Claims Trend: Ransomware

What's the **real damage** and how might a **cyber policy respond**?

- Payment of ransom → cyber extortion
- Forensic investigation → breach response
- Expense to restore data from backup → data protection
- Loss of business due to downtime → network business interruption
- Responding to regulatory inquiries → regulatory defense and penalties
- Individual third-party claims → information security and privacy liability

Claims Trend: Social Engineering

- What is social engineering? Method of attack that relies on human interaction to trick people into breaking normal security procedures.
    - o Phishing
    - o Spear phishing
    - o Whaling
    - o Smishing
    - o Phone calls
    - o Emails
    - o In-person
- What is social engineering used for?
    - o Funds transfer requests
    - o Requests for W2 and payroll records
    - o Installing malware
    - o Fraudulent tech support

HOW CEO FRAUD IMPACTS YOU

THE START

Attackers see if they can spoof your domain and impersonate the CEO (or other important people)

Bad guys often troll companies for months to gather the data necessary in pulling off a successful attack

THE PHISH

Spoofed emails are sent to high-risk employees in the organization

To: Finance Department

Urgent wire transfer request! Please send $100,000 to new acct #987654-3210

To: CFO

Please pay this time-sensitive invoice. I'm on vacation and will be unavailable, no need to respond. - Your CEO

To: Human Resources

I need a PDF copy of ALL employee W-2s for the IRS ASAP!

THE RESPONSE

Target receives email and acts without reflection or questioning the source

I better get this payment to the new account!

It's from the CEO, I'll take care of this for him!

Sounds important. I'll send these right away!

THE DAMAGE

Social engineering was successful, giving hackers access to what they were after

Causing fraudulent wire transfers and massive data breaches

THE RESULT

The fallout after a successful attack can be highly damaging for both the company and its employees

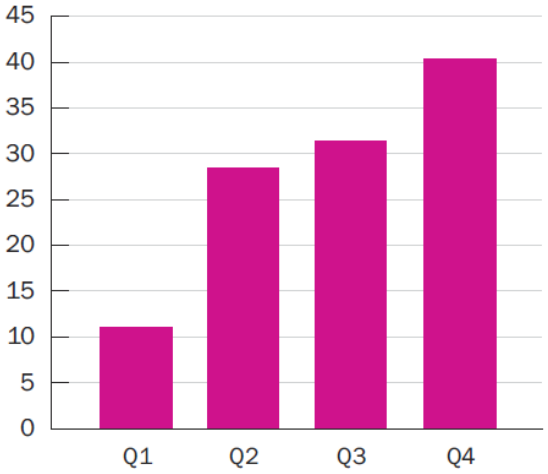
Resulting damage:

- ✓ Money is gone forever in most cases and only recovered 4% of the time
- ✓ CEO is fired
- ✓ CFO is fired
- ✓ Lawsuits are filed
- ✓ Intangibles - tarnished reputation, loss of trust, etc.

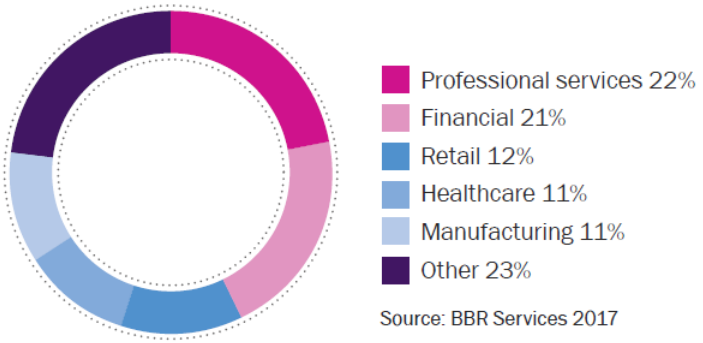
So... Think Before You Click!

Beazley 2017 Data

Fraudulent Instruction Incidents Reported to BBR Services, 2017



Fraudulent Instruction by Industry



Source: BBR Services 2017

What one company has done…

Residential Title & Escrow Company is proud to be a Baltimore City certified MBE/WBE

stewart
Vetted and verified.

WARNING! WIRE FRAUD ADVISORY

Wire fraud and email hacking/phishing attacks are on the increase! WE DO NOT ACCEPT OR REQUEST WIRING INSTRUCTIONS OR CHANGES TO WIRING INSTRUCTIONS VIA EMAIL. Always call 410-653-3400 to confirm. If you receive an email containing Wire Transfer Instructions, DO NOT RESPOND TO THE EMAIL! Instead, call your escrow officer/closer immediately at 410-653-3400 , using previously known contact information and NOT information provided in the email to verify the information prior to sending funds. This office will ALWAYS send wire information via encrypted email.

Claims Trend: Social Engineering

What's the **real damage** and how might a **cyber policy respond**?

- Fraudulent funds transfer
  - → Usually no coverage for the loss of money
  - → breach response (not in every case)
- Requests for W2 and payroll records
  - → breach response
  - → information security and privacy liability
- Installing malware → breach response
- Fraudulent tech support → breach response

Cyber liability and data breach

State of the market

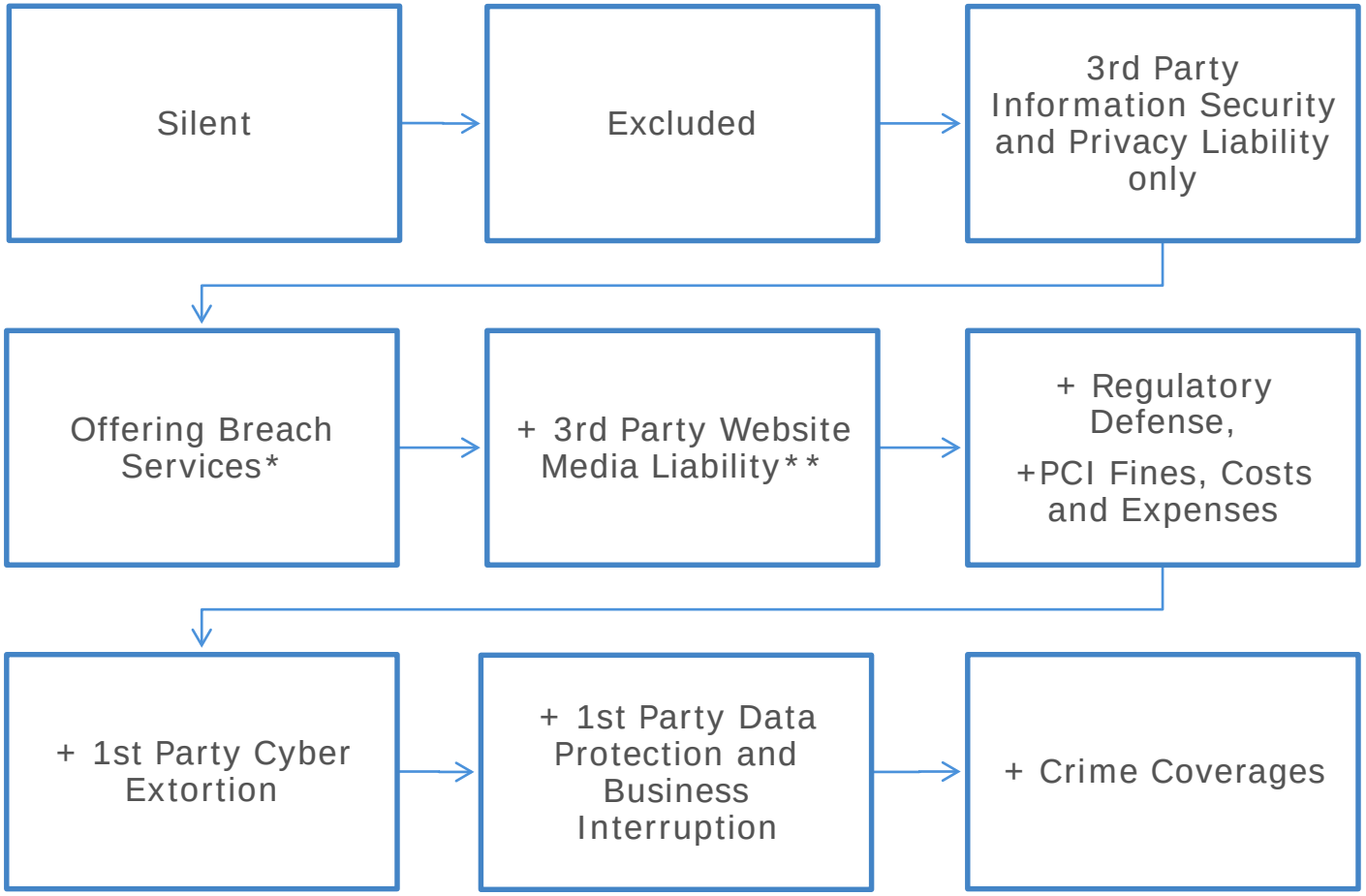
What is the Exposure to Risk?

What are common coverages?

Common Coverages?

- Nothing is common.
- Many company specific forms out there.
- Devil is in the details.

Coverage evolution



rapid exposure driven development

Typical Types of Coverages Are….

- Information Security & Privacy Liability Coverage
- Regulatory Defense & Penalties Coverage
- Website Media Content Liability Coverage
- Payment Card Industry (PCI) Fines, Expenses & Penalties Coverage
- Cyber Extortion Loss Coverage
- First Party Data Protection Loss Coverage
- First Party Business Interruption Coverage
- Fraudulent Instruction
- Crime Coverage
- Computer Expert Services
- Privacy Counsel
- Notification Services
- Crisis Management and Public Relations Services
- Credit Monitoring Services

Product Features

- Triggers for Breach Response Services
  - The industry has very tight triggers on breach response coverage.
  - Does the policy address require the breach, discovery and report all be within the policy period?
- How is terrorism handled?
- Are corporate records included?
- Are paper records covered?
- Are acts that occurred before the policy period covered?
- How is contingent BI handled?
- Does the policy come with risk management?
  - Website/Information Portal
  - Hotline
  - Pre breach services

THANK YOU

Libby.Benet@Beazley.com