

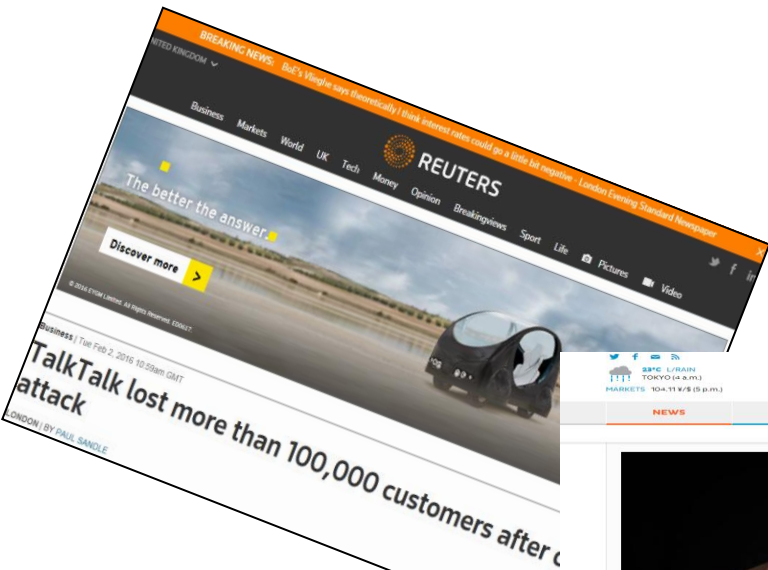


## Evolution of Cyber Risk and Its Impact on Insurance

6<sup>th</sup> Reinsurance Meeting of Rio De Janeiro

April 6, 2017





**REUTERS**  
The better the answer.  
Discover more

### TalkTalk lost more than 100,000 customers after attack

Business | Tue Feb 2, 2016 10:58am GMT  
LONDON (BY PAUL SANDE)



**The Japan Times NEWS**

### JTB hack underscores need for revamp of cybersecurity in Japan

NATIONAL  
BY ALAGSIAH WARDHANI  
STAFF WRITER

A massive data breach at Japan's largest travel agency has underscored the risks companies face when they keep sensitive data on networks connected to the internet. | ISTOCK

A massive data breach at Japan's largest travel agency has underscored the risks companies face when they keep sensitive data on networks connected to the internet, experts say. Some warn government systems are especially

JUN 16, 2016  
ARTICLE HISTORY



**mondaq**  
Connecting knowledge & people  
Employment | Real Estate | Commercial | Family | Finance | Government | Litigation | IP | Privacy

### Australia: Mandatory data breach notification is coming to Australia

Updated: 13 December 2015  
By Philip Catania and Tim Lee  
Philip Westgarth

The Australian Government released an exposure draft of its long-awaited notification bill, the [Privacy Amendment \(Notification of Serious Data Breaches\)](#).



**SC MAGAZINE**  
FOR IT SECURITY PROFESSIONALS  
NEWS | PRODUCT REVIEWS | BLOGS

### Malware campaign discovered targeting Latin America for 7 years

Danielle Correa  
December 11, 2015

Share this content: [Facebook] [Twitter] [LinkedIn] [Google+]

A seven-year long malware campaign has been discovered to be targeting several Latin American



**International Business Times**  
News | World | Business | Politics | Technology | Science | Sport | Entertainment | Opinion | Lifestyle

### Man Police Uncover Data Theft Involving 18 Emails and Passwords

IBT VIDEO

Advertisement (0:31)

EU charges God... dominance of A...

## DARKReading

Join us live at **blackhat Interop ITX**

Authors Slideshows Video Tech Library University Radio Calendar Black Hat News

**ANALYTICS** **ATTACKS / BREACHES** **APP SEC** **CAREERS & PEOPLE** **CLOUD** **ENDPOINT** **IoT** **MOBILE** **OPERATIONS**

## ATTACKS/BREACHES

4/4/2017  
10:20 AM



**Kelly Jackson Higgins**  
News

Connect Directly



**0 COMMENTS**  
[COMMENT NOW](#)

[Login](#)



## Cybercriminals Seized Control of Brazilian Bank for 5 Hours

**Sophisticated heist compromised major bank's entire DNS infrastructure.**

KASPERSKY SECURITY SUMMIT 2017 – St. Maarten – Cybercriminals for five hours one day last fall took over the online operations of a major bank and intercepted all of its online banking, mobile, point-of-sale, ATM, and investment transactions in an intricate attack that employed valid SSL digital certificates and Google Cloud to support the phony bank infrastructure.

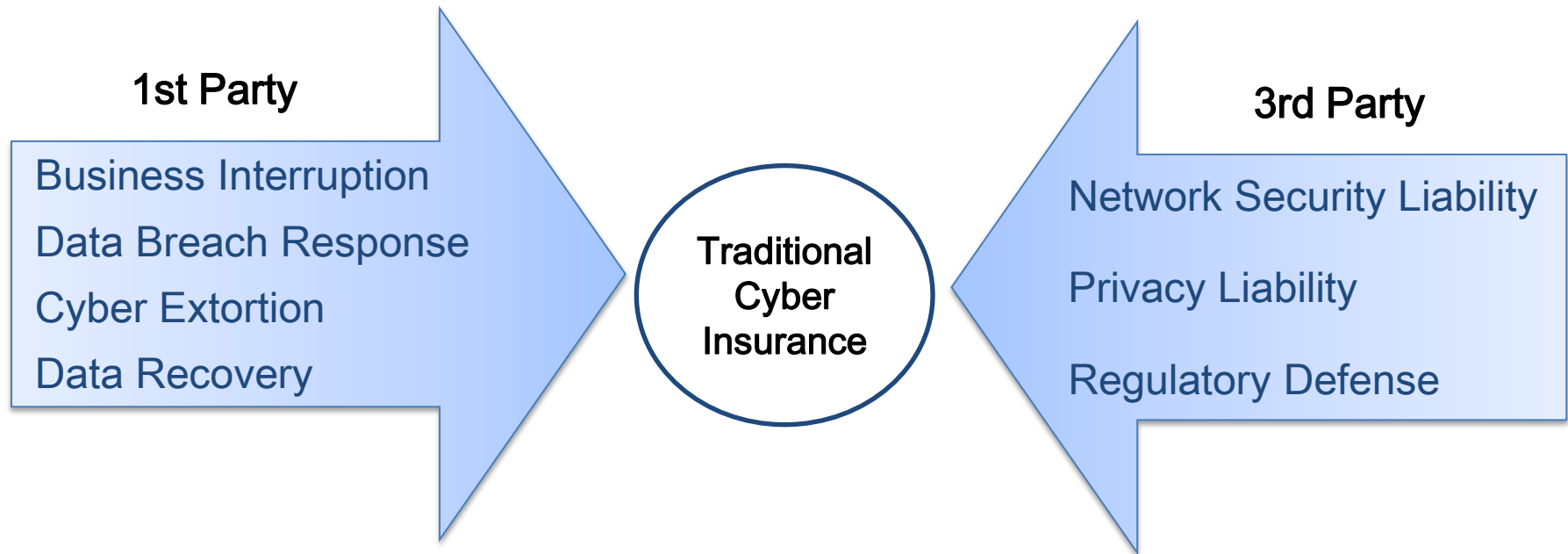
The attackers compromised 36 of the bank's domains, including its internal email and FTP servers, and captured electronic transactions during a five-hour period on Oct. 22, 2016. Researchers estimate that hundreds of thousands or possibly millions of the bank's customers across 300 cities worldwide, including in the US, may have been victimized during the hijack window when customers accessing the bank's online services were hit with malware posing as a Trusteer banking security plug-in application. The malware harvested login credentials, email contact lists, and email and FTP credentials, and disabled anti-malware software on the victim's machine to avoid detection.

- In recent years, Internet use has grown faster in Latin America than in any other region in the world<sup>1</sup>
- Combine with developing LATAM economies that are increasingly technologically savvy<sup>2</sup>



According to Inter-American Development Bank, LATAM faces cybercrime losses estimated at **US\$90B** a year

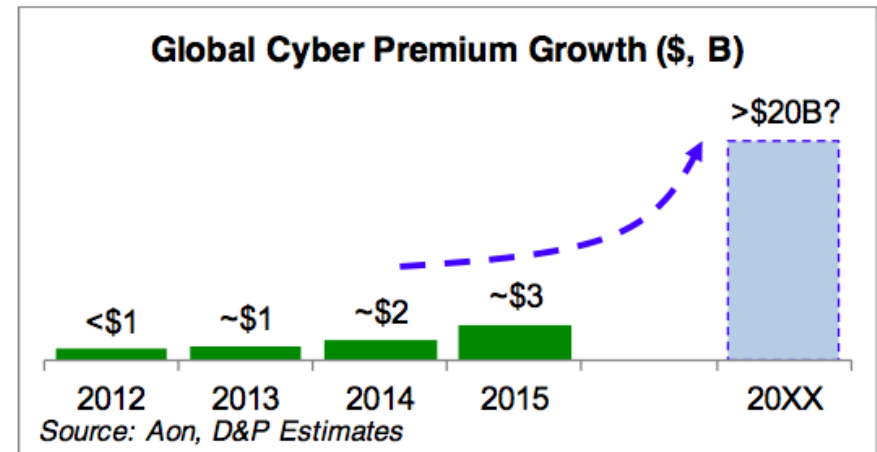
Source: 1 XL Catlin February 2016, 2 Kaitlin Lavinder – The Cipher Brief



- Product has been around ~ 18 years
- Evolved from Tech E&O product
- Claims-made policy form
- Underwriting use of third party analytics
- Short to medium tail in nature
- No standard form in market
- Vendor response services critical
- Written on standalone basis or blended

## Continued Growth

- 2016 Premium Estimate: **\$3.5B-\$4.5B**
  - Mostly U.S.
  - ~\$500M Europe
  - \$10-\$15M Latin America
  - Asia Pac emerging
- More industries purchasing
- Companies of all sizes purchasing
- Companies purchasing more limits
- Evolving regulatory requirements
- Third party requirements
- Top concern of Boards
- More data being created and stored
- Business interruption growing concern
- 60+ carriers in U.S. market (a lot of supply)
- Coverage broadening
- Enhancement in modeling and data analytics



Dowling and Partners: “One of few growth markets in the P&C industry”  
PWC anticipates \$7.5B premium by 2020,  
Allianz estimates \$20B by 2025

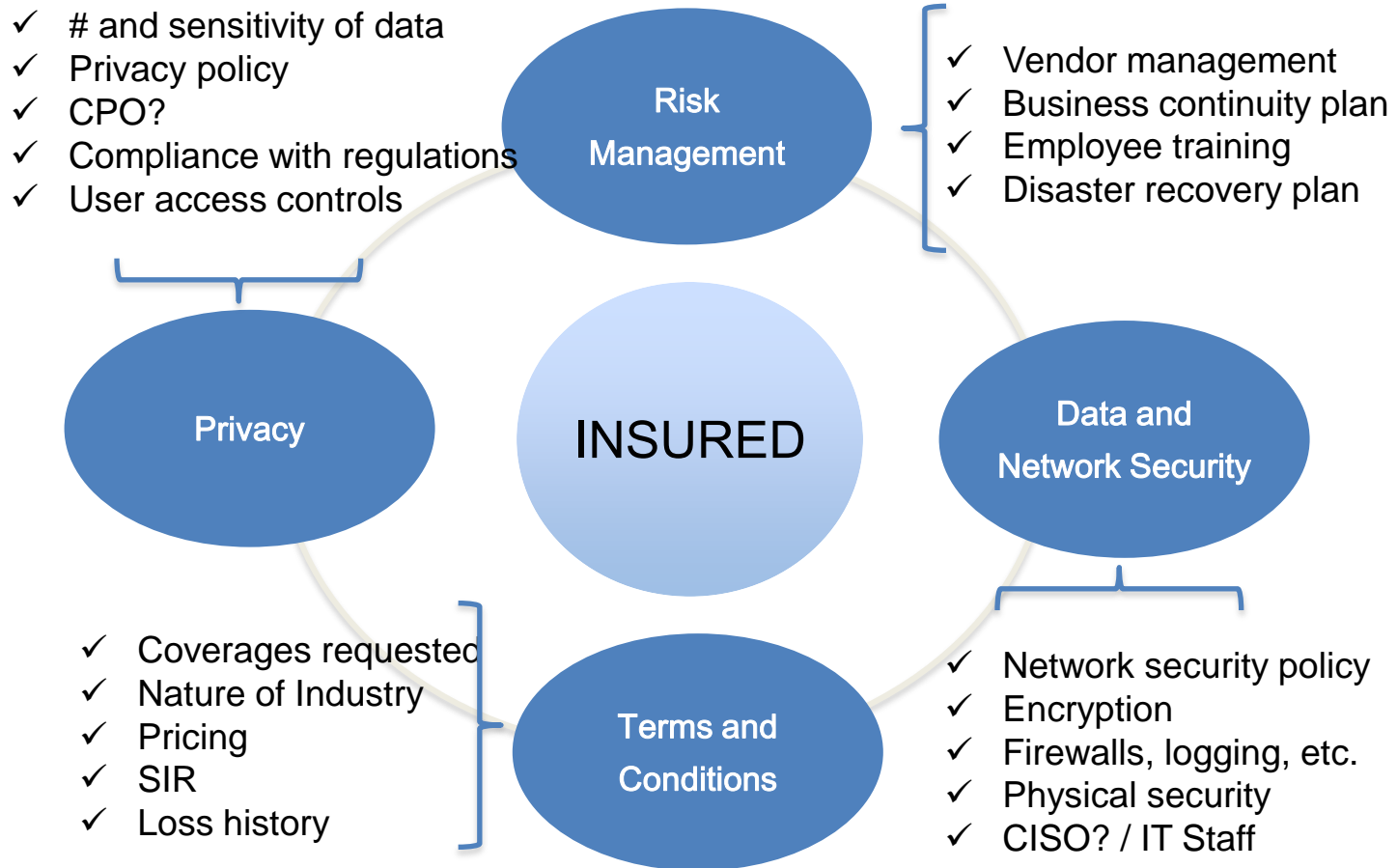
## Early Stages

- Carriers: AIG, XL Catlin, Allianz, Chubb, Liberty, SURA, Travelers Brazil
- Limits: up to \$10M (\$5M more common maximum limit)
- Financial Institutions, airlines, government entities purchasing
- Overall litigiousness low
- Lack of common framework regarding Data Protection
  - 4 out of 5 countries do not have cybersecurity protection plans in place<sup>1</sup>

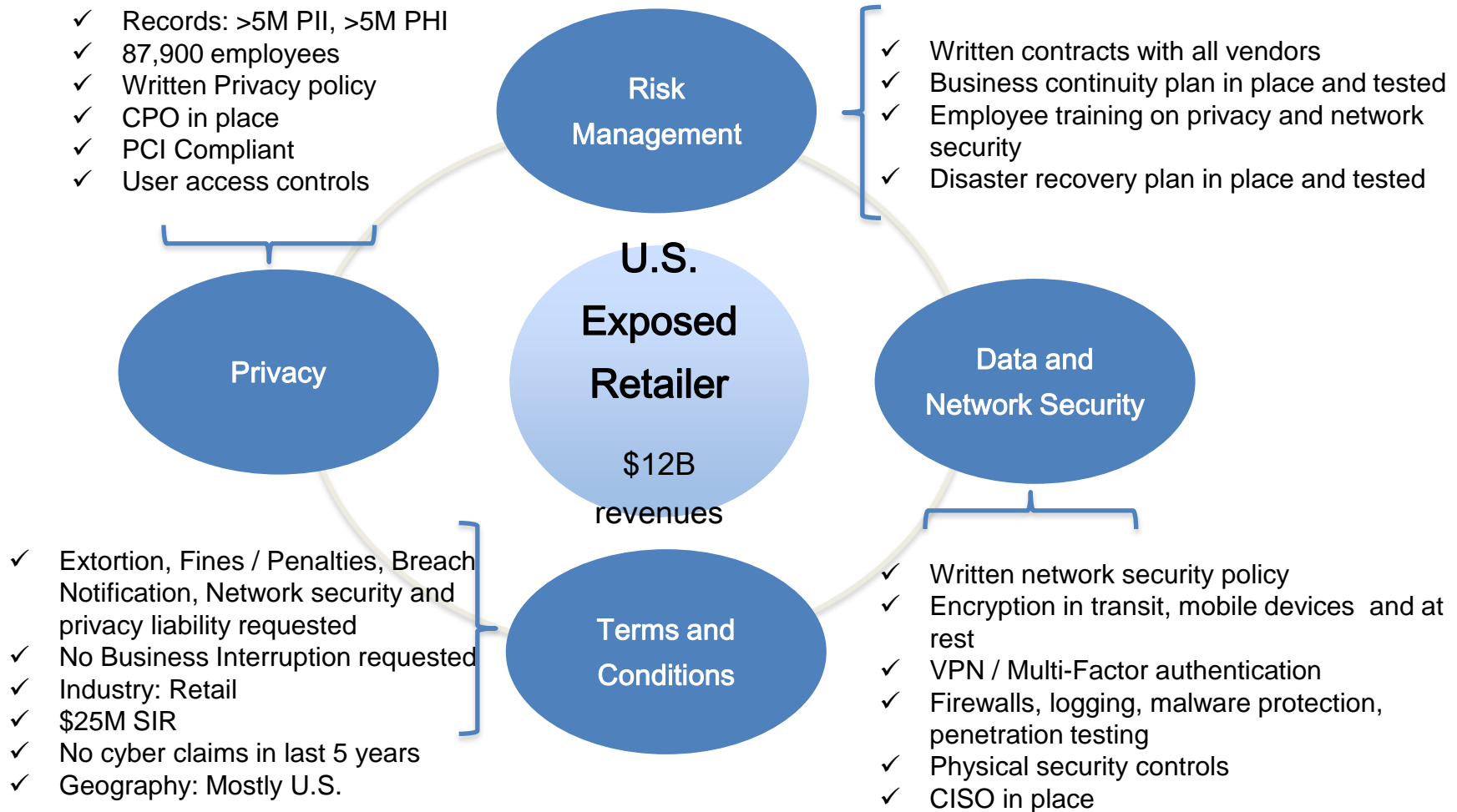
## Expect Increase in Demand

- 11% of business in LATAM hit by a cyber attack in past 12 months<sup>2</sup>
- Brazil saw 197% year-over-year increase in cyberattacks in 2015
- Increase in number of countries establishing regulations
- Companies are becoming more aware of cyber exposures (Mossak Fonseca)





- Difficult classes include Public Entities, Utilities, Energy, Social Networking, Higher Education, Large Retail, Healthcare, Payment Card Processors, Adult Websites, etc.




● \$65M limits requested, 8 carriers


# Cyber Risk is Systemic


 Directors & Officers (financial consequences following IT/cyber security failure)


 General/product liability

 Cyber Insurance

 Cyber liability insurance (no BI cover)

 PI E&O (third party financial losses)

 Cyber crime (first party restoration/exortion)

 Loss (Liability) of Financial and Personally Identifiable Data

 Non-physical damage business interruption

 Engineering extension

 Property extension

 Denial of Services Interruption of Operations (non-physical damage)

 Marine

 Aviation

 Casualty

 Engineering

 Property

 Cyber Attack on Critical Infrastructure (physical damage)

Source: CRO Forum Report – “Cyber Resilience – The Cyber risk challenge and the role of insurance”

## Numerous areas potentially exposed in the event of a cyber-attack:

- ✓ Loss of Intellectual Property
- ✓ Property damage
- ✓ Business interruption
- ✓ Reputational damage
- ✓ Fines/penalties/regulatory actions
- ✓ Bodily injury
- ✓ Extortion
- ✓ Breach of contract
- ✓ D&O and transactional liability
- ✓ Product liability and recall
- ✓ Stock drops, loss of profits
- ✓ Costs to notify/breach response costs
- ✓ Lost data
- ✓ Loss of monies transferred

“Cyber attacks may stem from a wide array of actors, affect all industries and result in varying levels of damage to data, critical systems, physical property, and even disrupt business continuity. For this reason, cyber risks can trigger a variety of insurance solutions.”

Source: CRO Forum Report – “Cyber Resilience – The Cyber risk challenge and the role of insurance”

Aggregation  
concerns

Changing  
technology

Educational  
gap

Coverage  
broadening

IT talent  
shortage

Treatment of  
terrorism

Lack of  
historical data

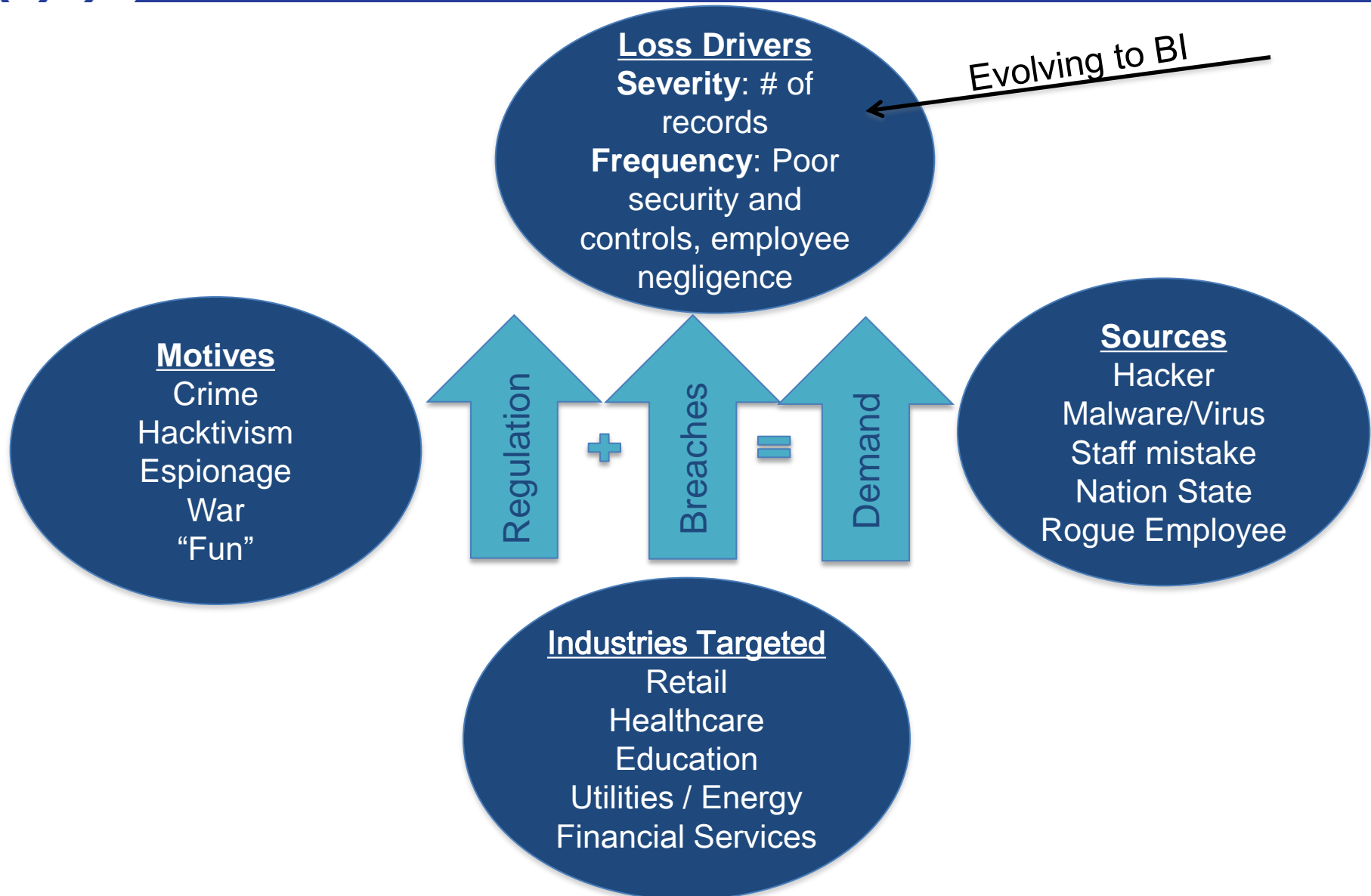
Increased and  
evolving  
regulation

Insurance  
talent shortage

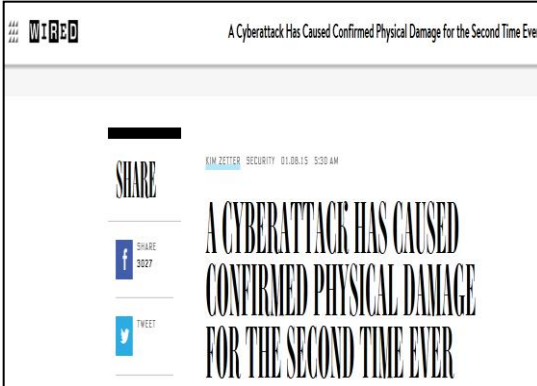
Sophistication  
of hackers

Inconsistent  
case law

Lack of  
catastrophic  
events



## Physical Damage on the Rise?



A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever

SHARE

KIM ZETTER SECURITY 01.08.15 5:00 AM

A CYBERATTACK HAS CAUSED CONFIRMED PHYSICAL DAMAGE FOR THE SECOND TIME EVER

## Increase in Attacks against Critical Infrastructure



CNN Money U.S. + Business Markets Tech Media Personal Finance Small Biz Luxury stock tickers

Cyber-Safe

Hackers attacked the U.S. energy grid 79 times this year

## Airline System Failures



REUTERS July 20, 2016, 4:18 PM

Southwest Airlines computer outage grounds fleet nationwide

A Southwest Airlines jet comes in to land at Lindbergh Field in San Diego, California February 25, 2015.

Comment / Share / Tweet / Stumble / Email

Last Updated Jul 20, 2016 11:05 PM EDT

CHICAGO -- Southwest Airlines flights across the country were held up

## Growth in Ransomware Attacks



22 Hospital Declares 'Internal State of Emergency' After Ransomware Infection

MAR 18

A Kentucky hospital says it is operating in an "internal state of emergency" after a ransomware attack rattled around inside its networks, encrypting files on computer systems and holding the data on them hostage unless and until the hospital pays up.

www.methodshospital.net

Internal State of Emergency due to a computer virus. Click here for additional information.

Method Hospital is currently working in an Internal State of Emergency due to a Computer Virus that has limited our use of electronic services.

1305 North Elm Street Henderson, Kentucky 42420 270-827-7700

Method Hospital awarded Magnet™ recognition

## Rise in Social Engineering



07 FBI: \$2.3 Billion Lost to CEO Email Scams

The U.S. Federal Bureau of Investigation (FBI) this week warned about a "dramatic" increase in so-called "CEO fraud," e-mail scams in which the attacker spoofs a message from the boss and tricks someone at the organization into wiring funds to the fraudsters. The FBI estimates these scams have cost organizations more than \$2.3 billion in losses over the past three years.

In an alert posted to its site, the FBI said that since January 2015, the agency has seen a 270 percent increase in identified victims and exposed losses from CEO scams. The alert noted that law enforcement globally has received complaints from victims in every U.S. state, and in at least 79 countries.

A typical CEO fraud attack. Image: Phishme

CEO fraud usually begins with the thieves either phishing an executive and gaining access to that individual's inbox, or emailing employees from a look-alike domain name that is one or two letters off from the target company's true domain name. For example, if the target

## Internet of Things Hacks



theguardian

pinion sports soccer tech arts lifestyle fashion business travel environment

DDoS attack that disrupted internet was largest of its kind in history, experts say

Dyn, the victim of last week's denial of service attack, said it was orchestrated using a weapon called the Mirai botnet as the 'primary source of malicious attack'

Major cyber attack disrupts internet service across Europe and US

Advertisement

See lowest prices from 200+ sites

Four Seasons Resort and...

**Bodily Injury**

**Mobile Apps**

**Telematics**

**Physical Damage**

**Internet of Things**

**Biometrics**

**Aviation & Marine**

**Social Engineering**

**Critical Infrastructure**

**Supply Chain Risk**

**Cloud Computing**

**Ransomware**

**Cyber Terrorism**





- Global cyber team with four dedicated individuals
- Committee with 22 representatives from various product lines, divisions, regions
- ERM is key – extreme event scenarios, aggregation tools, risk tolerances, referrals, tracking across product lines, portfolio management



*For your cyber treaty and facultative needs across the globe...*



*We value risk.*

*Nous apprécions le risque.*

*Wir schätzen Risiko.*

**Kara Owens**

Global Head of Cyber Risk

T: (1) 212 365 2129

E: [kowens@transre.com](mailto:kowens@transre.com)

**Lauren Markowski**

AVP, Cyber Risk

T: (1) 212 365 2301

E: [lmarkowski@transre.com](mailto:lmarkowski@transre.com)

**Rhett Hewitt**

AVP, Cyber Risk

T: (44) 20 7204 8676

E: [rhewitt@transre.com](mailto:rhewitt@transre.com)