Cyber Insurance Landscape
Catherine Rudow
November 2017
The following presentation is for general information, education and discussion purposes only, in connection with the CAGNY Fall 2017 Meeting of the Casualty Actuarial Society. Any views or opinions expressed, whether orally or in writing are those of the speaker alone. They do not constitute legal or professional advice; and do not necessarily reflect, in whole or in part, any corporate position, opinion or view of PartnerRe or its affiliates, or a corporate endorsement, position or preference with respect to any issue or area covered in the presentation.
Cyber Insurance Landscape – What shapes the insurance marketplace?

- Hacker Motivations
- Regulation
- Losses
- Aggregation Potential in Cyber
- Cyber Insurance Market Forces – Supply vs Demand
- Risk Mitigating Factors
- “Silent Cyber”
Hacker Motivation
Hacker Motivation
Verizon Data Breach Investigations Report (DBIR) 2017

Figure 3: Threat actor motives over time

http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017
Shift in Threat Actions

Figure 4: Percentage of breaches per threat action category over time

Regulation
Cyber Liability – Regulatory and Statutory Landscape

Federal Requirements

• **FTC** (Federal Trade Commission)
  • FACTA (Fair & Accurate Credit Transactions Act)
  • Gramm-Leach-Bliley Act

• **HIPAA** (Health Ins Portability and Accountability Act) governs use and disclosure of PHI
  • HITECH (Health Information Technology for Economic and Clinical Health Act)
  • Office of Civil Rights (OCR) responsible for enforcing the HIPAA Privacy and Security Rules
Cyber Liability – Regulatory and Statutory Landscape

• State Requirements – 48 states, DC, Guam, PR and the Virgin Islands have compulsory notification laws in place
  • Excludes entities covered by the HITECH Act
• Breach notification laws vary from state to state
• All states maintain that the owner of data is responsible for the breach
EU General Data Protection Regulation (GDPR)

- Protects the privacy of all personal data collected on EU citizens.
- Personal data is broadly defined
- Applies to all responsible parties that hold personal information on EU citizens
- Expected to become law May 2018
- Backed by heavy financial penalties
Losses

Data Breach
Denial of Service
Ransomware & Destructive Malware
Social Engineering
PartnerRe Cyber Liability Market Trends Survey - 2017

What do you see as the top driver(s) of Cyber product sales? (Choose up to three)

- News of cyber-related losses experienced by others: 80%
- Experiencing a cyber-related loss: 60%
- Increased education: 50%
- Required by a third party (e.g., customer): 40%
- Board or senior management demand: 30%
- Cost: 20%
- Breadth of coverage: 10%
- Good sales people: 5%
- Risk mitigation services: 5%
- Other: 0%
DATA BREACH

• LOSSES DRIVEN BY
  • Hacker Motivations
  • REGULATION

• Aggregation Potential

• Claims Costs
  • Notification costs
  • Credit monitoring
  • Forensics
  • Fines and Penalties
Target (late 2013) – Market Maker?

- Involved Phishing, vendor, and POS malware
- 70M individuals affected (40M+ CCs)
- Affected 4th QTR sales
- CEO fired
- Followed by a succession of other retailer breaches in 2014
- Sped adoption of microchips in US
- Recently settled with 47 states for $18.5M

PartnerRe Cyber Liability Market Trends Survey - 2017

What Cyber coverages are NEW and RENEWAL buyers most interested in purchasing? (Please select top three)

Data Breach: Equifax (2017)

- This breach was preventable – Data Breach lasted ≈3 months
- Exposed highly sensitive data of 143M people
- Hack has hallmarks of nation-state role – Information not yet on black market?
- CEO has stepped down/early retirement of 2 top security officials (CIO and CSO)
- FTC is investigating – Several lawsuits have already been filed.

- *May impact other lines, i.e. D&O*
DENIAL OF SERVICE ATTACK (DoS or DDoS)

Losses Driven By:

- Hacker motivation usually not financial (unless DoS used as extortion)
- Generally a tool for cyber warfare/attack

Aggregation Potential

Claims Costs:

- Business Interruption
- Contingent Business Interruption
Denial of Service Attacks (DoS)
Distributed Denial of Service Attacks (DDoS)

A cyber attack that renders a machine or a network unavailable to users, usually by bombarding it with “requests” that overloads it.

As we become more dependent on the internet, DDoS attacks can pose a serious threat. Main insurable loss here is business interruption.
“The size of these DDoS attacks has increased so much lately thanks largely to the broad availability of tools for compromising and leveraging the collective firepower of so-called Internet of Things devices — poorly secured Internet-based security cameras, digital video recorders (DVRs) and Internet routers.”
Internet of Things (IoT)

IoT is the network of physical items (devices, vehicles, buildings, etc.) that are embedded with electronics, software, sensors, or actuators that have network connectivity and can collect and send/receive data. (Wikipedia)

Examples:

- Security cameras
- Nest Thermostat
- Medical Devices e.g. Pacemaker
- Fitbit
September 2016 – Hijack Video Cameras

- Attackers used an army of as many as one million Chinese made security cameras and video recorders to launch several massive internet attacks that knocked their targets offline.
- Affected sites in France (web hosting provider OVH) and US (security researcher Brian Krebs).
- Use of botnet/malware Mirai. Identifies devices with weak security.

October 2016 – The Dyn DDoS Attack

• The attacks – there were three, in relatively quick succession, aimed at the Dyn’s managed Domain Name Server (DNS) infrastructure. (Dyn.com)

• Reports indicate that Dyn provides service to more than 1,200 domain names.

• Among the websites that experienced issues as a result of the attack are Reddit, GitHub, Spotify, Twitter, Imgur, PayPal, Wired, Netflix, Etsy, Amazon and Yelp. Wikipedia.org

• **Source of attack is Mirai botnet.** (Dyn.com)
RANSOMWARE & DESTRUCTIVE MALWARE

Losses Driven by:

• Hacker Motivation

Aggregation Potential

Claims Costs:

• Cyber extortion demands
• Forensics
• Business Interruption
• Contingent Business Interruption
Ransomware – CryptoWall (Kaspersky Lab Study)

- Attacks against the corporate sector 2015-2016 has grown six fold from last year (from 27,000 to 158,000)
- More frequent attacks, targets small and mid-sized
- Crypto malware is a serious threat, involving money for ransom and paralyzing businesses during the recovery period.
- Most Famous: Hollywood Presbyterian (until recently)
  - In February, hackers infected computers
  - Demand 17K (40 Bitcoin)
  - Caused disruption for several weeks
Trend Micro Report: The Reign of Ransomware

• In first half of 2016, discovered 79 new ransomware families
  • JIGSAW ransomware deletes a number of files for every hour the ransom isn't paid. SURPRISE, another ransomware variant, increases the ransom amount if the user fails to meet the deadline.

• Raimund Genes, chief technology officer for Trend Micro noted: "It has dominated the threat landscape so far in 2016, causing immense losses to businesses across multiple industries."

2017 Ransomware

Cerber ransomware – evolved to evade detection by machine learning solutions

Patcher – a MacOS ransomware

Growth of new ransomware families plateaued in first half of 2017 – criminals focusing on diversifying in terms of potential victims, platforms and bigger targets. New ransomware tactics, techniques and procedures (TTPs) are emerging!!
WannaCry May 2017

- Attacked older Windows based systems – exploit is known as “EternalBlue” and released by Shadow Brokers online in April
- Used a worm component allowing to spread without user interaction
- Spread was prevented by a killswitch – found quickly or would have been more widespread

https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

- It made $140K – don’t know who perpetrators are, but linked to Lazarus group (North Korean Government)

https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware
‘Wannacry’ ransomware attacks

Worldwide attack has crippled more than 300,000 computers in 150 countries

- Location of computers attacked by the ‘WannaCry’ ransomware

Recorded by security blog MalwareTech in the 24 hours up to May 16, 00:00GMT

*Malicious software (malware) that encrypts files on an infected computer and demands payment to unlock them

- Attack started on May 12
- Attackers demand payment of $300 in virtual currency Bitcoin
- The virus uses a security flaw in Microsoft’s Windows XP operating system
- Hackers exploited NSA** software leaked earlier this year


© AFP
Impact of WannaCry attack

- Renault shut down several French factories after cyberattack
- Some Nissan UK factories affected
- Utilities in Spain
- UK’s National Health Service (was a mess for days)
- Universities in China (bootlegged software)
- Police in Andhra Pradesh, India
- Petrobras (Brazil state-owned oil company)

Estimated Economic damages from hundreds of millions up to $4B (Cyence estimate)

https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
New Breed of Ransomware/Malware in 2017 Causing Business Interruption

- NotPetya “Ransomware” Attack (June 2017) – deliberately engineered to damage IT systems.
  - NotPetya shares code with earlier ransomware called Petya, but much of it has not been seen before
  - Malware not designed to make money, but to permanently damage to the hard drive
  - Scraper Malware that is very destructive
  - Majority of infections are in Ukraine (60%) but affected multinationals that do business there.

Impact of “NotPetya” greater than “WannaCry”

This malware disrupted a number of large multinationals for weeks, disrupting their systems, and in many cases, affecting their financial outlook.

Companies affected include Maersk, Merck, FedEx, WPP (global advertising firm), DLA Piper (global law firm), Saint Gobain, Reckitt Benckiser (British consumer goods), and the list goes on...
CEO of A.P. Møller - Mærsk A/S, Søren Skou, states:

“In the last week of the quarter we were hit by a cyber-attack, which mainly impacted Maersk Line, APM Terminals and Damco. Business volumes were negatively affected for a couple of weeks in July and as a consequence, our Q3 results will be impacted. We expect that the cyber-attack will impact results negatively by USD 200-300m.”
Drug and vaccine maker Merck & Co Inc (MRK.N) said it suffered a worldwide disruption of its operations when it was the victim of an international cyber attack in June, halting production of its drugs, which will hurt its profits for the rest of the year.

https://www.reuters.com/article/us-merck-co-results/merck-says-cyber-attack-halted-production-will-hurt-profits-idUSKBN1AD1AO
FedEx

FedEx was the latest company to note that the “NotPetya” cyber attack on its TNT unit will continue to hurt revenues. According to FedEx the effects will be felt through the second fiscal quarter and full-year fiscal 2018 and force bigger IT investments.

Reuters.com
SOCIAL ENGINEERING – Funds Transfer Fraud

This is not a “hacking” loss

Do you believe funds transfer fraud loss due to social engineering fraud is better covered by a Cyber policy or a Crime policy?

The majority of respondents felt that funds transfer fraud coverage should be covered by the Crime policy, though this was largely driven by underwriter responses.
Social Engineering (Manipulation - Con)

- Phishing/Spear Phishing/Whaling
- Pretexting (uses invented scenario – elaborate lie)
- Baiting (relies on curiosity or greed of victim)
- Vishing (Phone Phishing)
- SMiShing (SMS Phishing - mobile device)
- Tailgating (following someone into a restricted area)
  - One example of social engineering is an individual who walks into a building and posts an official-looking announcement to the company bulletin that says the number for the help desk has changed. So, when employees call for help the individual asks them for their passwords and IDs thereby gaining the ability to access the company’s private information.
  
Social Engineering Example: “wire transfer scheme”

• Sophisticated emails that look routine/ordinary
• Works well in large organizations where may not know employees or customers personally
• Criminals send email that looks “right” and may even have fraudulent website to back up the email (in case employee clicks the link).
• Employee is duped into wiring money
• Where does coverage for this belong?
Aggregation Potential
Where does Aggregation Potential Come From?

• Vendors (e.g. payment processors)
• Widespread DoS Attacks – Business Interruption
• Widespread Ransomware Attacks - WannaCry
• Common vulnerability that can be exploited (e.g. WannaCry & NotPetya)
• Common Malware (e.g. Dridex)
• Affects other lines of business (e.g. D&O)
• Support multiple treaties writing same insureds
Have systemic events such as Dyn DDoS attack and WannaCry ransomware impacted underwriting and/or pricing?
Market Forces – Supply vs Demand
Cyber Insurance Marketplace
• 60+ markets offering coverage on stand-alone basis. Many more endorsing coverage on existing policies
  • Competitive market
  • Not standardized product (seeing some movement toward standardization as policy forms are being re-written)
• Limits up to $25M (Offered by about 10 markets)
• A few consortium/facilities able to offer up to $100M limits
• Market Capacity: $600M
• Coverages evolving to fit needs of insureds
  • Vendors and other third parties
  • Fines and Penalties
  • Social Engineering
What are the biggest obstacles to writing/selling this coverage? (Select up to three)
Market Size

- Estimated to be about $3.75B+
- Mostly US business – 90%
  - What will be impact of GDPR?
- Growth from new insureds
- Growth from increased limits

FOR 2017/18:

- Growth from expanding coverage
- New companies offering product

Expect 15%+ global premium growth in 2018
Are your renewal insureds requesting higher Cyber insurance limits?

- Frequently: 10%
- Sometimes: 60%
- Rarely: 20%
- Never: 5%
- Don't know: 5%
Have you seen Cyber business switch from endorsements to stand-alone policies?

Strong indication of buyers shifting from endorsements to stand-alone policies

Risk Mitigating Factors
Shoring up Security: Latest Bug Bounty Programs (2017)

- Samsung’s bug bounty program will pay up to $200K – program covers 38 mobile devices (Sept)

- Microsoft will pay up to $250K for Windows 10 security bugs (July)

Just about all major tech firms, auto manufacturers, the government, cloud providers, etc., have used a bug bounty program. They provide a legitimate way for hackers to make a living and help create less vulnerable software.
Helping understand our exposure: Aggregation Models

- There are several commercial aggregation models available
- Mainly deterministic (difficult to do probabilistic – but slowly moving in that direction)
- Models still in infancy
- Growing in sophistication
Insurance reduces costs of claims
NetDiligence Claims Study (2015)

• “Many insurers are leveraging legal counsel (Breach Coach®) early in the claims process to minimize mistakes on the part of the affected organization. This tends to prevent or minimize follow-on regulatory fines, legal defense and settlement costs.”

• Insurers are putting in place ‘preferred vendor panels’ with pre-negotiated rates for Crisis Services costs, which we believe significantly reduces the cost of breach response for policyholders of those insurance carriers. We estimate data breach response costs for an uninsured organization could be up to 30% higher than costs for an insured organization.

Important Role of Government Department of Homeland Security

• Combating cyber crime – works with other Agencies
• Involved with security Federal networks
• Very involved with Cybersecurity and critical infrastructure
• Working with Re/Insurers to protect critical infrastructure -
• Research and development
• Educate businesses and the public
• Information sharing
FBI (Federal Bureau of Investigation)

Lead Federal Agency for investigating attacks:

• Cyber Division (provides coordination)
• Cyber Squads (56 field offices)
• Cyber Action Teams (travel team dangerous cases)
• Computer Crimes Task Forces (93 of them)
• Partnership with other Federal Agencies, including DoD and DHS
Data Breach Investigations Report - 2016

Figure 9.
Breach discovery methods over time, (n=6,133).

**NIST Cybersecurity Framework** – National Institute of Standards and Technology - Department of Commerce

- Released in early 2014 – Updated in early 2017
- Designed for critical infrastructure (utilities, banks, etc) but can be used by all companies.
- Helps to manage supply chain risks, measurement methods for cybersecurity, and provides guidance to reduce risk.
- Has an established and defined vocabulary
- 30% US companies using framework (nist.gov)
Silent Cyber – the lines are blurring
German Steel Mill (2014)

- Penetrated the system through Phishing
- Hack into office software network
- Penetrated into production management software
- Took over control systems (ICS)
- Prevented blast furnace from doing its job resulting in an explosion and extensive damage to the plant

https://www.sentryo.net/cyberattack-on-a-german-steel-mill/
Medical Devices (Star Tribune, MN, 10/18/16)

- Today about 14 billion devices are connected to the internet, including some bedside drug-infusion pumps in hospitals and pacemakers implanted in patients' chests.

- In theory, a malicious hacker could compromise a device and then cause medical harm to a patient by causing an error in drug dosing or draining a device's battery, but no case of this happening has been documented.

- On Oct. 4, Johnson & Johnson announced cybersecurity vulnerabilities that would allow a person to remotely control a One Touch Ping insulin pump.
First IoT Lawsuit: Hello Barbie

- Claims talking Barbie invades children’s privacy, violating COPPA
- Users create an account with ToyTalk and register doll – permission required to activate doll’s speech processing
- Plaintiffs argue that Mattel does not protect privacy of children that are recorded, but do not own the doll (expectation that children will play with the doll with other children).
Cyber Insurance Products
Cyber Liability Insurance – FIRST PARTY "Core” Coverages

• Data Breach Response
  • Investigation, public relations, customer notification, credit monitoring

• Cyber Extortion

• Business Interruption
  • Can be specific to a security event or defined peril
  • Can be for *system failure*

• Contingent Business Interruption
  • Not necessarily standard
  • Can be for named vendors only/IT vendors only

PartnerRe
Cyber Liability Insurance – FIRST PARTY

• Electronic Media Liability (common)
• Data Restoration (common)
• Public Relations (common)

• Social Engineering Fraud
• Computer Systems Fraud
• Theft of Money or Securities
Cyber Liability Insurance – THIRD PARTY

PRIVACY LIABILITY
- Liability arising from loss or breach of the data

NETWORK SECURITY LIABILITY
- System failure
- Transmission of malicious code

Regulatory Fines and/or penalties and PCI (Payment Card Industry) fines and/or penalties
- Can be sub-limited
- Can be offered with endorsement
- Where insurable by law
Specialized Products/Facilities

- Very limited insurance for Intellectual Property losses
- Broader coverage on cyber policies offered for SMEs
  - Social Engineering
  - Reputational Harm

Broader coverage on cyber offering Property Damage

Broader coverage on cyber offering third party BI/PD

Broader coverage offering Business Interruption on property policy in absence of physical damage
Cyber Liability (Re)insurance Opportunities

• Still an expanding market
  • Becoming required coverage in some cases
• Market more sophisticated - adopt best practices
• Government involvement
• Response services more competitive = less costly
• Significant Vendor Activity that assists with underwriting, securing networks, pre-breach and post breach services

This exposure is not going anywhere! It is important to understand it, underwrite it, and price it!

PartnerRe
PartnerRe