Evolving Cyber Risk- A Multidisciplinary Perspective

Dr. Kathleen Locklear, MBA, D.Mgt.
Michael Solomon, FCAS, MAAA, CERA

ADMINISTRATIVE ITEMS

Antitrust Notice

- **The Casualty Actuarial Society is committed to adhering strictly to the letter and spirit of the antitrust laws. Seminars conducted under the auspices of the CAS are designed solely to provide a forum for the expression of various points of view on topics described in the programs or agendas for such meetings.**
- **Under no circumstances shall CAS seminars be used as a means for competing companies or firms to reach any understanding – expressed or implied – that restricts competition or in any way impairs the ability of members to exercise independent business judgment regarding matters affecting competition.**
- **It is the responsibility of all seminar participants to be aware of antitrust regulations, to prevent any written or verbal discussions that appear to violate these laws, and to adhere in every respect to the CAS antitrust compliance policy.**

Other "Housekeeping"

- Information presented today reflects the opinions of the presenters and its not intended to, nor should be, imputed to any of their employers.

Introduction to Session

- Learning Objectives
  - Understanding emerging risk in the cyber space
    - Deconstructing “emerging risk”
    - Cognitive/perceptual “ blind spots” and how those may impact decision making
    - Applications/implications for insurance
      - Capacity
      - SIRs/Deductibles
  - Rethinking emerging risk in the cyber arena

Introduction to Dr. Kathleen Locklear

- Adjunct Professor at University of Maryland, University College
  - Dissertation: “Emerging Risk: A Systems Thinking and Complexity Approach”
  - Research Interests: emerging risk, systems thinking, complexity theory, risk perception
- Senior Director, Global Insurance – Teva Pharmaceuticals
  - Worlds largest generics pharma producer; $ 19.7 B revenue (FY 2015)
- RIMS Strategic Risk Management Committee Member

Introduction to Michael Solomon

- FCAS, MAAA, CERA
- 1st Prize, Society of Actuaries/ Casualty Actuarial Society Joint Risk Section Cybersecurity call for Essays
- 1st Prize, Professionally Speaking Toastmasters public speaking competition
- CAMAR Vice President
- Member, Committee for P&C focused ERM Seminars
- Member, CAS/ CIA/ SOA Impairment Project Oversight Group

INTRODUCTION

Some Cyber Losses

Breach	Cause	Cost (Ground Up)	Cost (Insured)
Epsilon	Spear-Phishing[i]	Up to $4 billion[ii]	No coverage in place
Home Depot	Vendor Cybersecurity Failure and Microsoft Windows security failure	$ billions[iii]	$100 million
Wendy's	Unknown	$ billions[iv]	Unknown
Veterans Administration	Computer/ External Hard Drive incidentally stolen from employees house during burglary[v]	$500 million[vi]	No coverage in place
Target	Vendor Cybersecurity Failure	$252 million[vii]	$90 million
Hannaford Bros	Malware	$252 million[viii]; ID theft insurance and replacement card costs held compensable[viii]	No coverage in place
Sony Playstation	Unknown	$171 million[viii]	Unknown; settlement when appeal pending after bench granted summary judgment against Sony[ix]
TJ Maxx	Poorly Secured Wireless LAN in two stores[x]	$256 million[xi]	$19 million[xii]
Sony Pictures Entertainment	North Korea	$151 million + reputation	$151 million
Heartland Payment Systems	SQL Injection attack[xiii]	$140 million[xi]	$30 million[xiv]
Anthem	Bogus Domain Name/ Phishing	Over $100 million[xi]	$100 million[xv]

Evaluating Coverage- Current Practice and Thinking

- Pricing
- Terms/Conditions
  - SIRs/ Deductibles
  - Limits
  - Scope of Cover
  - Covered Events
  - Coverage Triggers

Emerging Risk

"We also know there are known unknowns; that is to say, we know there are some things we do not know.
But there are also unknown unknowns – the ones we don't know we don't know."

United States Secretary of Defense, Donald Rumsfeld
Press Briefing, February 12, 2002

Category 1~ Framing the Problem

- Things we don't know… but we're aware of it!
  - Emerging Risk as an "information gap"
  - Solutions:
    - Ask others
    - Fill in the data points, gaps

Category 2~ Framing the Problem

- Things we don't know… and we're unaware of it!
  - Much more difficult
  - NOT merely an information gap that can be filled
  - Emergent nature presents specific challenges and limitations

Category 2~ A Closer Look

(Things we don't know… and we're unaware of it!)

- Emerging risk~ "A novel manifestation of risk, of a type that has not been experienced before" (Locklear, 2011)
  - **Pure**- never experienced before, at all, by anyone
    - example: nanotechnology, fracking, genetically modified crops
  - **Hybrid**- blends together known risk types in new ways (combinations) to produce outcomes that haven't been experienced before
    - Example: Zoonotic disease + global warming = (zika?)
    - Example: Overstressed power grids + greater dependence on telecommunications + {X Factor} = ???

Challenges of Emerging Risk

- 'Relational Complexity': Growing difficulty in determining relationships among causal factors, making risk more 'opaque'
  - Richardson, Cilliers & Lissack (2001)
    - Under these conditions, causes and effects no longer have simple, linear connections
    - It's more difficult to ascertain interactions between elements
    - Implication: Challenges for appropriately pricing and structuring insurance where "cause" (i.e.- "trigger, for insurance) is not always apparent

Challenges of Emerging Risk

- Amplification/Cascade potential: Seemingly simple root causes can trigger events which cascade through a network and are amplified to produce an extreme event
  - Example: August 2003 mega-power outage
    - Ohio, Maryland, New York, Toronto
    - Overstressed lines failed in Ohio after contacting overgrown tree limbs (Holbrook, 2010)
    - Expected outcome was a minor, local outage
    - Implication: Appropriate pricing for insurance, as well as capacity, are challenged when a seemingly minor event is amplified

Challenges of Emerging Risk

- Emerging risk is often opaque, clouded within a complex web of causal factors, until it escalates into an extreme event
  - In an environment of great complexity, emerging risk may remain "hidden" (latent)
  - Modern structures, like the "Internet of Things" provide rich environments for this period of latency
  - Implication: Insurance/risk management need to use different tools
    - Environmental scanning can help identify early "signals of change" (Ashley & Morrison, 1997) which if overlooked, ignored or downplayed, can allow emerging risk to continue along its development trajectory

Challenges of Emerging Risk

- May involve rapid and widespread deployment of new/novel technology/modalities
- By the time an issue is identified, the problem is already extensive

"Classic" Example of Emerging Risk

- Asbestos ("Emerged" risk)
  - Naturally occurring, used as far back as ancient Greece
  - Industrial revolution, insulator for furnaces
  - Subsequently used far and wide
  - Then problems grew apparent (1960's)
  - Extensive litigation, ongoing abatement problems
  - Classic illustration of unexpected impact for insurers

  - NOTE: Hind-sight is 20/20!

Challenges of Emerging Risk

- Lack of historical data OR data that is not entirely relevant
  - The capabilities of traditional risk management tools (quantitative, predictive) are being stretched when applied to emerging risk
    - Traditional modeling does not "fit" the challenges of "unknown-unknowns"
    - Implications: In order to optimize approaches, including insurance, "non traditional" tools may be needed
      - Environmental scanning, systems thinking

Our "Human" Challenges

- Tendency to focus within the "comfort zone"
  - Risks that are well known, well understood
  - Lots of data available for analysis
  - "Pure" risks that either happen, or don't (e.g.- fire), with no up-side potential
- We tend to heavily value corroborating factual information and discount outliers, non-conforming information

More "human" challenges

- Recent movie "Everest"

- Roberto, M. A. (2002). Lessons from Everest: The interaction of cognitive bias, psychological safety, and system complexity. *California Management Review, 45*(1), 136-158.

"Human"challenges- Lessons from the movie 'Everest'

- Commitment escalation- continuing to invest resources, commitment to a course of action that increasingly appears questionable at best (Staw, 1987)
  - Led climbers to ignore rules and place themselves in increasing danger

- Recency bias- tendency to focus on more recent events
  - Hindered the judgment of the expedition leaders who had experienced good weather on Everest during the prior recent years, causing them to underestimate the severity of the storm **despite historical data that showed the conditions on May 10, 1996 were anything but abnormal.**

More "human" challenges

- Groupthink
  - Defective decision making that occurs when conformity pressures of a group lead to faulty decisions, made in an effort to preserve group harmony.
  - Defective 'groupthink' decision making is characterized by the following attributes: poor information searching; selective bias in information processing; incomplete surveying of objectives and alternatives; failure to re-examine choices and rejected alternatives; and failure to develop contingency plans (Janis & Manning, 1977, p. 132).
- "a disease of insufficient search for information, alternatives and modes of failure" (McCauley, 1998, p. 144)

Something to Consider: Lessons from the Black Swan (Taleb, 2007)

- Extreme outlier (unpredictable)
- Thought not to exist (improbable)
- Outside the boundaries of "normal" expectations
- It can't be… therefore it isn't

Futurist thinking- Emerging risk in the cyber realm

CONCEPTUALIZING EMERGING CYBER RISK

- CYBER COPE™ FRAMEWORK
- "FOOD FOR THOUGHT"
- SCADA
- HACKING OF MEDICAL DEVICES
- HACKING OF DRIVERLESS CARS

COPE- APPLICATION TO CYBER

- COPE- construction, occupancy, protection, exposures
  - Each category represents a set of data points
  - Used to evaluate combined property risk for a structure/building

COPE applied to cyber/technology to create Cyber COPE™ (Cohen, 2016)

Summary of COPE to Cyber-COPE™

COPE	CYBER COPE™	MEASUREMENT TYPE	SAMPLE DATA ELEMENTS
CONSTRUCTION	COMPONENTS	OBJECTIVE	NUMBER OF ENDPOINTS, NETWORK CONNECTIONS, SOFTWARE VERSIONS, DATA CENTER LOCATIONS
OCCUPANCY	ORGANIZATION	OBJECTIVE	POLICY HOLDER'S INDUSTRY, QUALITY OF IT/SECURITY RELATED POLICIES, USE OF INDUSTRY STANDARDS

Retrieved October 27, 2016 at https://www2.chubb.com/us-en/business-insurance/transforming-cyber-underwriting.aspx.

Summary of COPE to Cyber-COPE™

COPE	CYBER COPE™	MEASUREMENT TYPE	SAMPLE DATA ELEMENTS
PROTECTION	PROTECTION	SUBJECTIVE	DATA RETENTION POLICIES, FIREWALLS, MONITORING, INCIDENT RESPONSE/READINESS POLICIES
EXPOSURES	EXPOSURES	SUBJECTIVE	POLITICAL OR CRIMINAL MOTIVATION, TYPES OF OUTSOURCING, TYPE/AMOUNT OF SENSITIVE INFORMATION

Retrieved October 27, 2016 at https://www2.chubb.com/us-en/business-insurance/transforming-cyber-underwriting.aspx.

Hacking in action- Use of smart phones

- Max Cornelisse, Netherlands
  - hacking train schedule board
  - turning building lights on/off
  - raising/lowering drawbridge
  - changing digital highway road sign
  - Videos available on YouTube
  - Real, not real?

SCADA

- Supervisor Control and Data Acquisition
  - Refers to industrial control systems (ICS)
    - Computer systems that monitor and control industrial, infrastructure or facility-based processes
    - System collects data from various sensors at factory, plant or other remote locations
    - Sends data to central computer that manages and controls the data

Possible SCADA Hacking Scenarios

- Power outages (blackouts, across grids)
- Waste water mixed with drinking water
- Disruption of manufacturing lines
- Transportation disruption/shut down

- NOTEWORTHY
  - Potential for impact far away from the compromised source itself
  - Amplification of impact
  - Cascade effect

Actual SCADA Incidents

- Thirteen assembly lines shut down at Daimler-Chrysler, Zotob worm, 2005
- Springfield, Illinois public water supply pump burned out after being cycled on and off repeatedly (November 2011) through an IP address in Russia

Actual SCADA Incidents

- Ohio Davis-Besse nuclear power plant safety monitoring system off line for 5 hours, January 2003, Slammer worm
- Brisbane hacker used radio transmissions to create raw sewage overflows on Sunshine coast (2000)
- CSX Transportation computers infected by virus (August 2003) halting train traffic in Washington, D.C.

Emerging threats to critical infrastructure

- A computer virus attacked a turbine control system at a U.S. power plant
  - A third party technician had unknowingly used an infected USB drive on the network
  - Plant was down for three weeks

Insulin Pump Hacking

- **"J&J Warns Insulin Pump Vulnerable to Cyber Hacking"**
  - **October 4, 2016, Wall Street Journal**
- OneTouch Ping uses unencrypted radio signal
- Hacker in close proximity could use equipment to detect signal and program the device

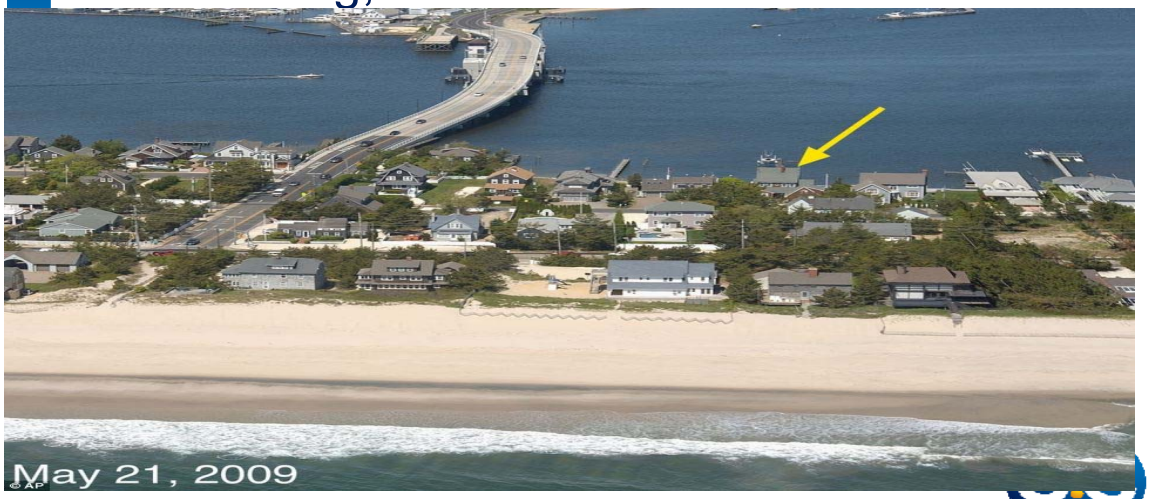
Driverless Car Technology

- Apps to unlock doors, start cars
  - "Now is the transitional period, and it's kind of ugly. They're old-school industries. They were mechanic or electronic kinds of systems, and now they're software-based companies—and they haven't realized they're software-based companies, and that's sort of the problem."
    - Craig Smith, founder of Open Garages http://www.vocativ.com/332734/driverless-car-hack/ (June 29, 2016)
    - DECISION ALGORYTHMS TO AVOID CRASHES
      - SACRIFICE DRIVER TO SAVE GROUPS OF PEOPLE

Concluding thoughts-

- Some lessons from Super Storm Sandy… on a personal note

Before …
Mantoloking, NJ



After …

Super Storm Sandy

- Worth thinking about
  - Some flood zone maps haven't been updated in over 30 years
    - NYC FEMA map last updated 1983
  - Unintended consequences of coastal replenishment after other storms? (emerging risk)
  - "Only" a Cat 1 storm and not a classic "named storm"

Conclusion

- "The task is not to get it right but to get it less wrong, not to disprove existing understandings but to recognize their context-dependence, not to discover what is, but to construct from conflicting understandings previously unconceived alternative understandings." Grobstein, 2010

Concluding Q&A

Suggested Readings

- Ariely, D. (2008). *Predictably irrational: The hidden forces that shape our decisions*. New York: Harper Collins.
- Bazerman, M.H. & Watkins, M.D. (2004). *Predictable Surprises: The disasters you should have seen coming and how to prevent them*. Boston: Harvard Business School Press.
- Friedman, T.L. (2005). *The world is flat: A brief history of the twenty-first century* (1st ed.). New York, NY: Farrar, Straus and Giroux.
- Haeckel, S.H. (2004). *Peripheral vision: Sensing and acting on weak signals- Making meaning out of apparent* noise. *Long Range Planning,* 37(2), 181-189.
- Hubbard, D.W. (2010). *How to measure anything: Finding the value of intangibles*. Hoboken, NJ: John H. Wiley & Sons.
- Taleb, N.N. (2007). *The black* swan. New York, NY: Random House