The Institutes
CPCU Society

4A Security & Compliance

CAS

USING NEW DATA SOURCES IN THE CYBER INSURANCE UNDERWRITING PROCESS

CAS CPCU Underwriting Collaboration Seminar
New Orleans, LA
June 27, 2018

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.

Ben Goodman, CRISC

Ben Goodman, Founder & CEO of 4A Security & Compliance

- Affiliations
  - Faculty Member, Drexel University, LeBow College of Business
  - Distinguished Fellow of the Ponemon Institute
  - Member, Casualty Actuarial Society, Cyber Risk Task Force
  - Advisory Board Member, Pace University Seidenberg College of Computing, Cybersecurity Institute
  - Member, National Cyber Healthcare Working Group
  - Member, ISACA, Infragard, ISSA, OWASP
- Awards
  - Best Paper, Joint CAS/CIA/SOA, Practical Risk Management Applications
  - Worldwide Achievement Award, ISACA CRISC

ABOUT 4A SECURITY

Founded in 2012

Leadership

Leadership team has 20+ Years each of IT, Security & Risk Management experience.
Team holds CISA, HCISSP, CRISC, CISSP, CEH, and other security, IT and risk mgmt. certifications

Clients range from global public companies to venture-backed tech start-ups.

Developer of CyRisk – A cyber risk analytics tool enabling insurance carriers, reinsurers and cyber risk managers gain visibility into silent cyber and cyber aggregation risk in their portfolios.

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

Audience Poll

Work in Cyber:

1. Main part of job
2. Minor part of job
3. No part of job

Audience Poll

In Analysis, do you break out Cyber from other coverages:

1. Yes
2. No
3. N/A

Audience Poll

Do you mainly rely on:

1. Frequency-Severity Methods
2. Other Methods
3. Benchmarks (e.g. Me-too filings)
4. N/A

Audience Poll

How confident are you (1 = low, 5 = high) in your pricing & underwriting, relative to other lines (e.g. GL)

1. 1
2. 2
3. 3
4. 4
5. 5
6. N/A

Audience Poll

Have you used commonly available, free, cyber-data (e.g. Ponemon Study, CyberSecurity Coverage Supplement, Others' rate filings)

1. Yes
2. No
3. N/A

Audience Poll

Have you purchased specific cyber-data for your work?

1. Yes
2. No
3. N/A

Audience Poll

If asked, would you recommend aggressively growing this book (above and beyond current clients, or with GL business, without policy limits under $100,000):

1. Yes
2. No
3. Sitting on Fence

AGENDA

- Audience Poll
- Introduction
- Cyber Risk Data – Value & Limitations
  - Historical Cyber Incident Data
  - Outside-In Cyber Data
  - Inside-Out Cyber Data
- Cyber Risk Data and Accumulation Risk
- Audience Poll Follow-up

INTRODUCTION

What is your primary source of data when underwriting a prospective cyber risk?

INTRODUCTION

INTRODUCTION

What is your primary source of data when underwriting a prospective cyber risk?

INTRODUCTION

What is your primary source of data when underwriting a prospective cyber risk?

1. Cyber Application?
2. Underwriting call?
3. Security industry reports?
4. Compliance/certifications?
5. Comparable insureds/Market price?
6. Market share?

INTRODUCTION

What is your primary source of data when underwriting a prospective cyber risk?

- Cyber Security Scores?
- Cyber Security Assessments?
- Other?

INTRODUCTION

DATA CHALLENGES

- Variability of exposure base by industry class and by coverage
  For example:
  - Revenue
  - Record count

INTRODUCTION

DATA CHALLENGES

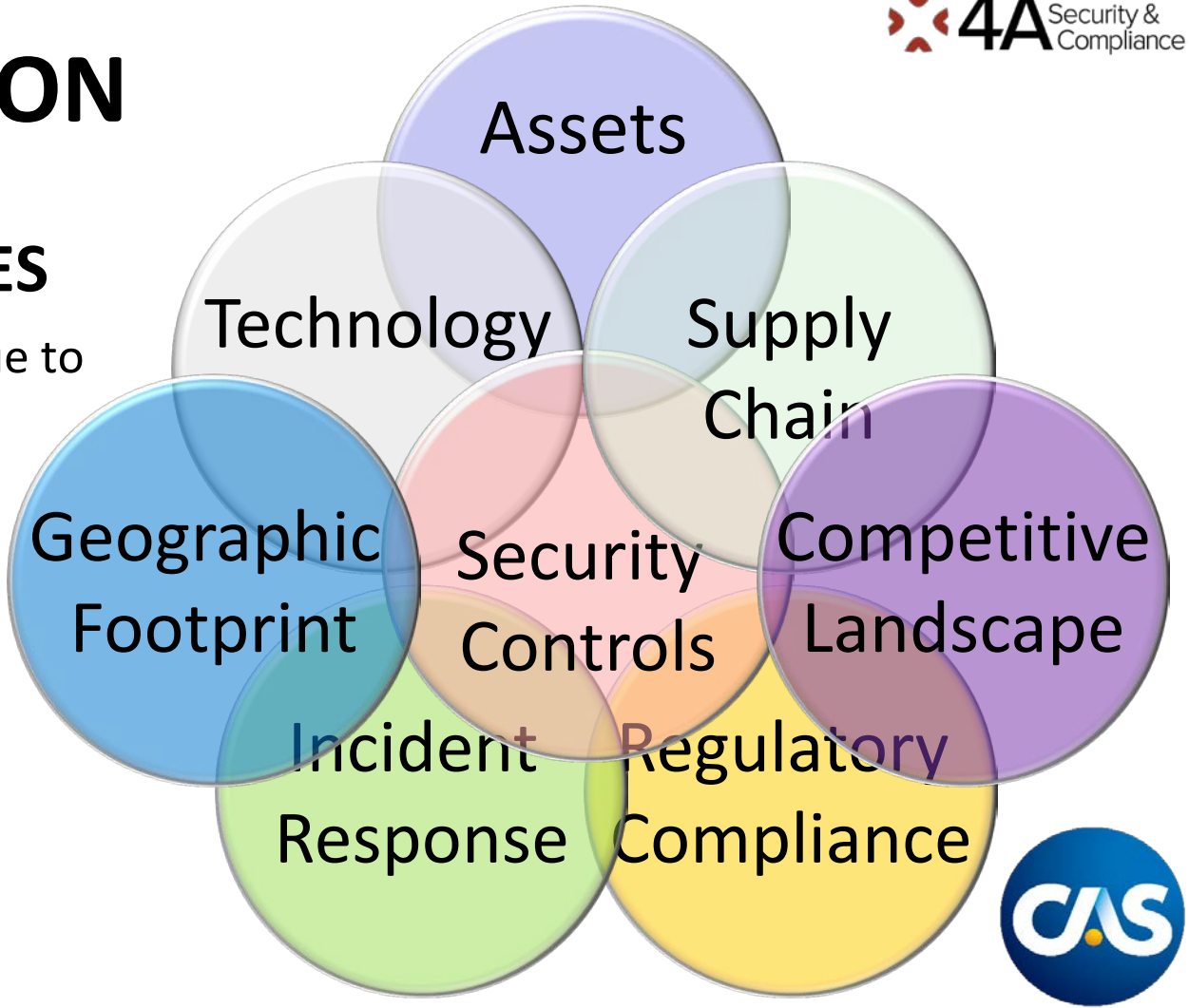
- Market share analysis vs. detailed analysis*
  - Dyn scenario analysis
    - Correct ~20% of the time
    - Underestimation of 50% or more also 20%
  - CBI scenario analysis
    - 32% (or higher) difference between market share and detailed analysis

** Cloud Down, Impacts on the US economy, Emerging Risk Report 2018 – Technology; Lloyds 2018*

INTRODUCTION

DATA CHALLENGES

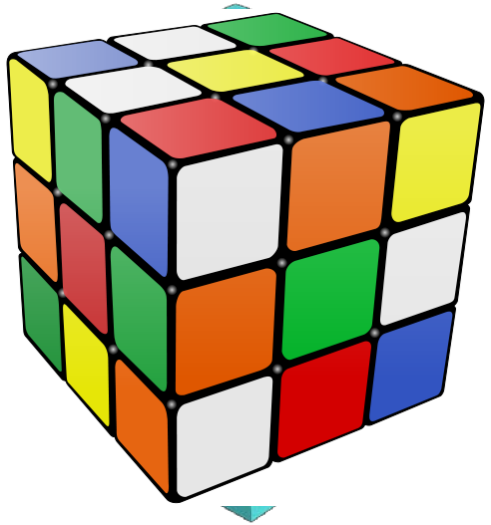
- Incomplete picture due to
  - Lack of visibility
  - Fragmented views

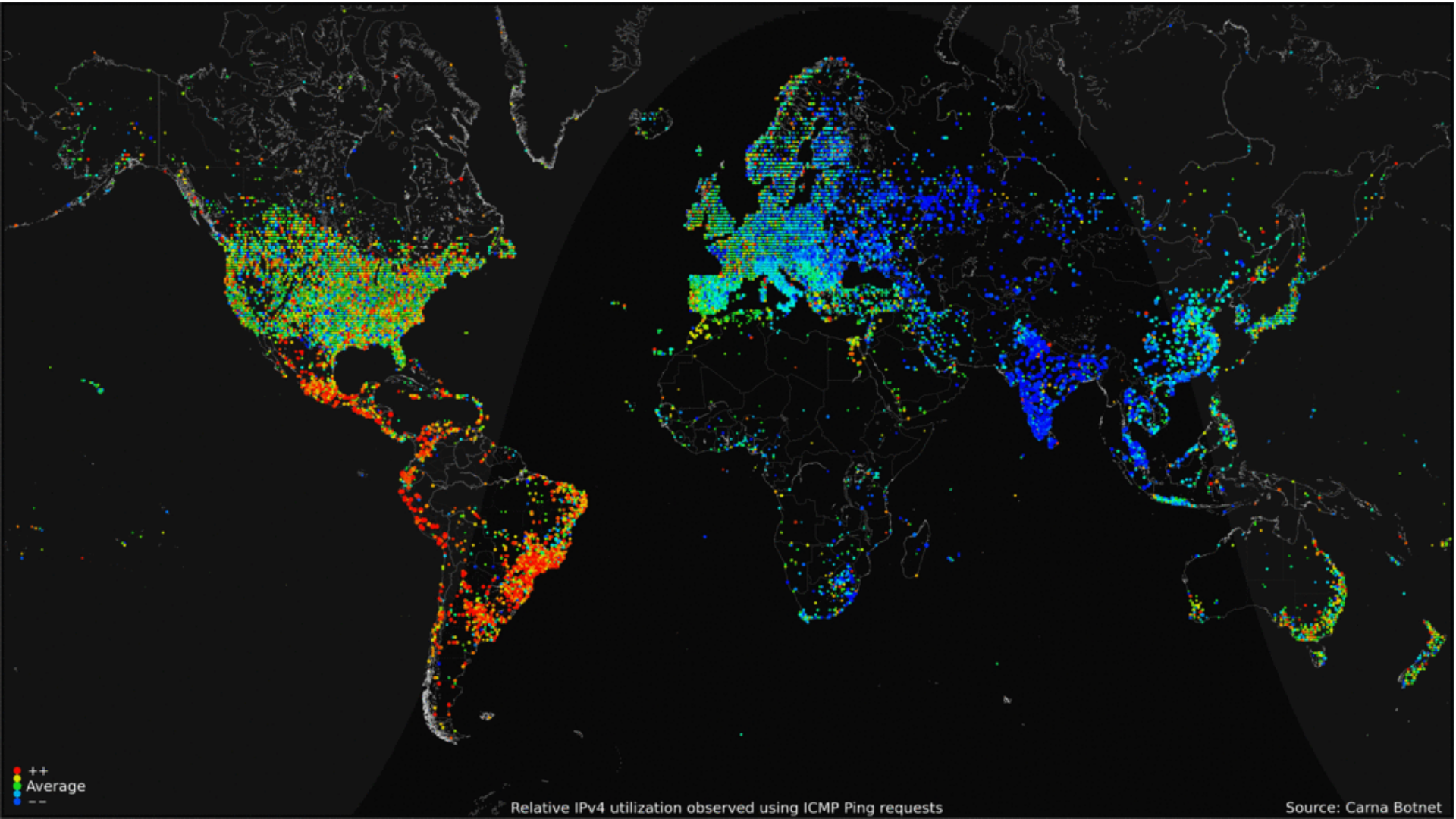


INTRODUCTION

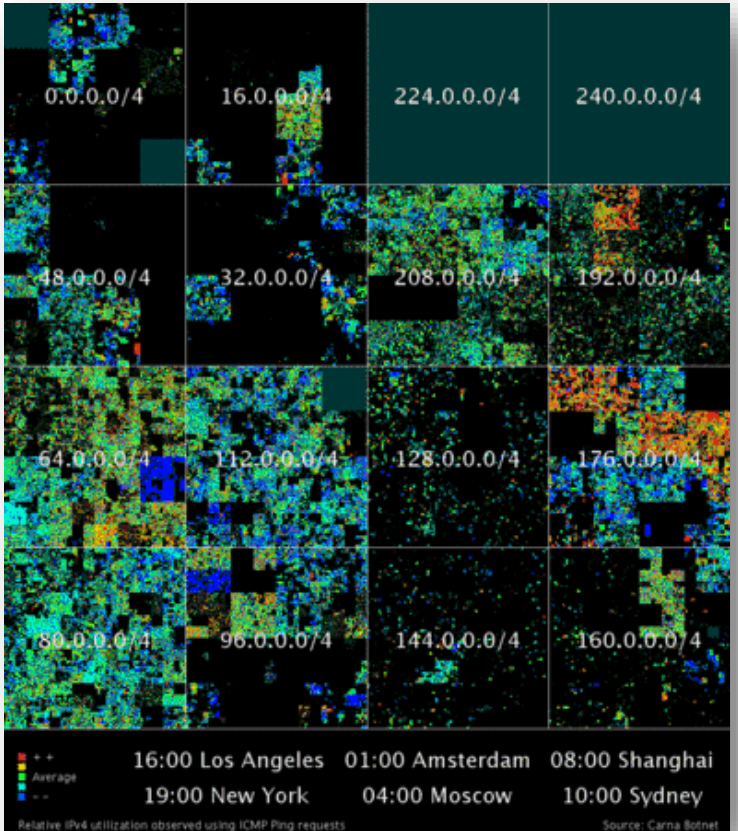
DATA CHALLENGES

- Cyber risk is rapidly changing on many levels
  - Threat landscape
  - Security controls
  - Technological infrastructure
  - Business innovation
  - Insurance coverage

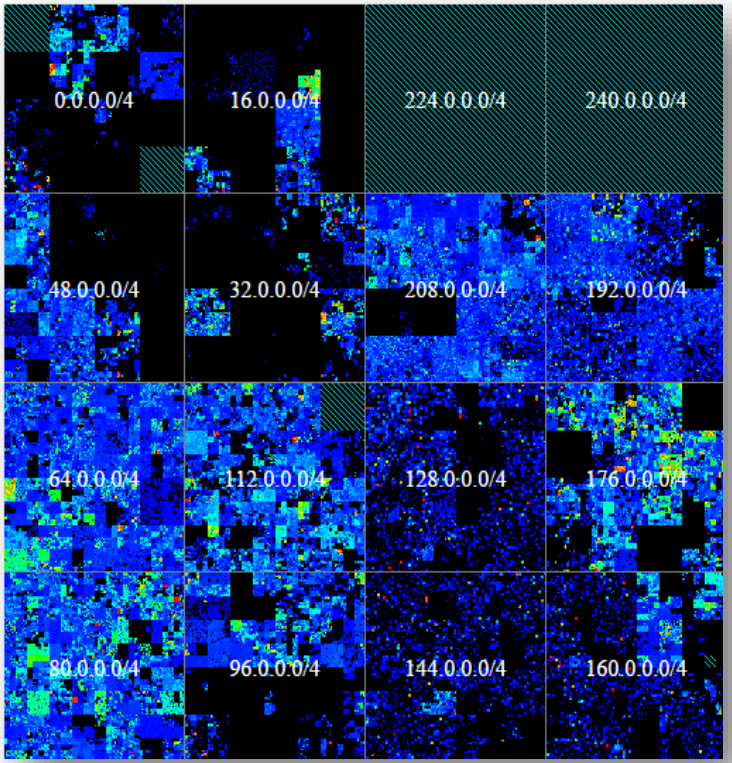



++
Average
--
Relative IPv4 utilization observed using ICMP Ping requests
Source: Carna Botnet

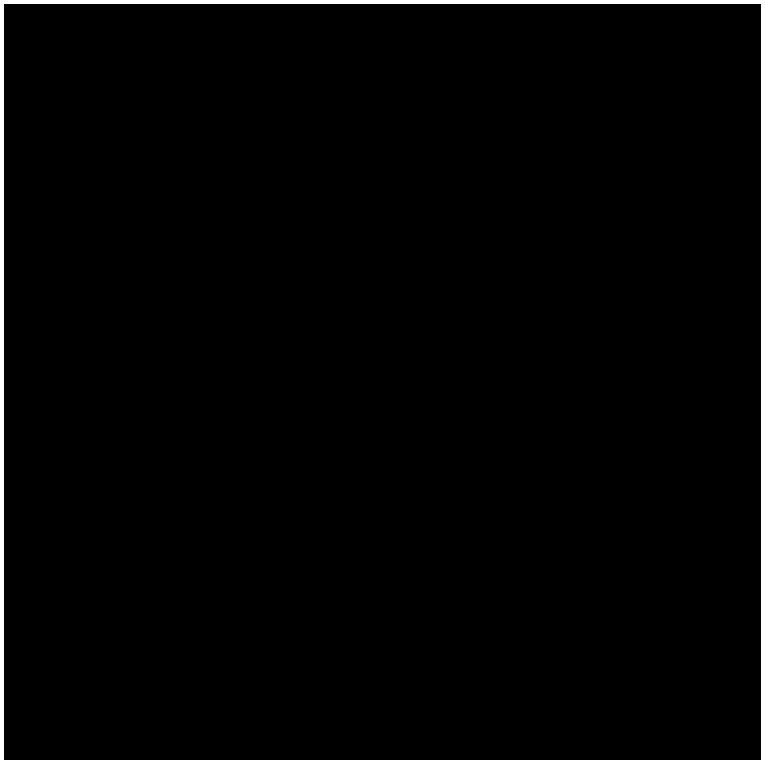
CYBER RISK DATA



CYBER RISK DATA

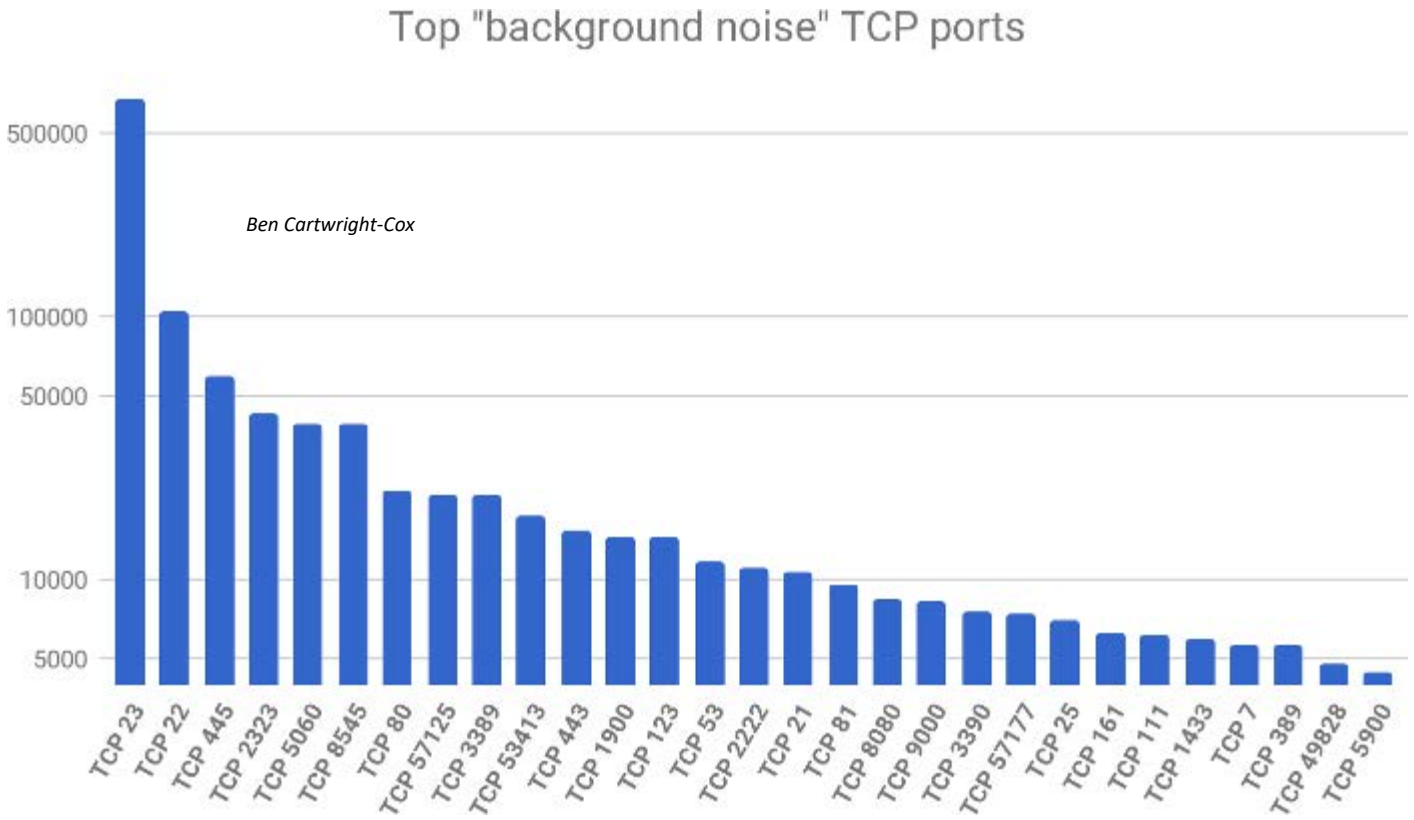


CYBER RISK DATA



IPv6

CYBER RISK DATA



CYBER RISK DATA

Coverages

- Incident Response Costs
- Forensics
- Notification
- Credit Monitoring & Identity Restoration
- Regulatory & Legal Defense Fees
- Fines And Penalties
- Media Liability
- Directors & Officers Liability
- Reputational Damage
- Intellectual Property Theft

CYBER RISK DATA

Coverages

- Business Interruption (1st party & dependent)
- Physical Asset Damages
- Bodily Injury and Death
- Cyber Ransom and Extortion
- Data / Software / System Loss

- Financial Theft / Fraud (BEC)

Availability
Integrity

CYBER RISK DATA

Factors include:

- Dynamic threat landscape
- Threat actors and motivations
- Targeted vs. opportunistic attacks
  - Targeted attacks lend themselves to scenarios / attack tree modeling
  - Opportunistic (spray and pray) attacks lend themselves more to probabilistic modeling
- Security interdependencies and risk propagation

CYBER RISK DATA

CYBER RISK DATA SOURCES

- Historical Cyber Incident Data
- Outside-In Cyber Data
- Inside-Out Cyber Data

HISTORICAL CYBER INCIDENT DATA

CYBER RISK DATA SOURCES

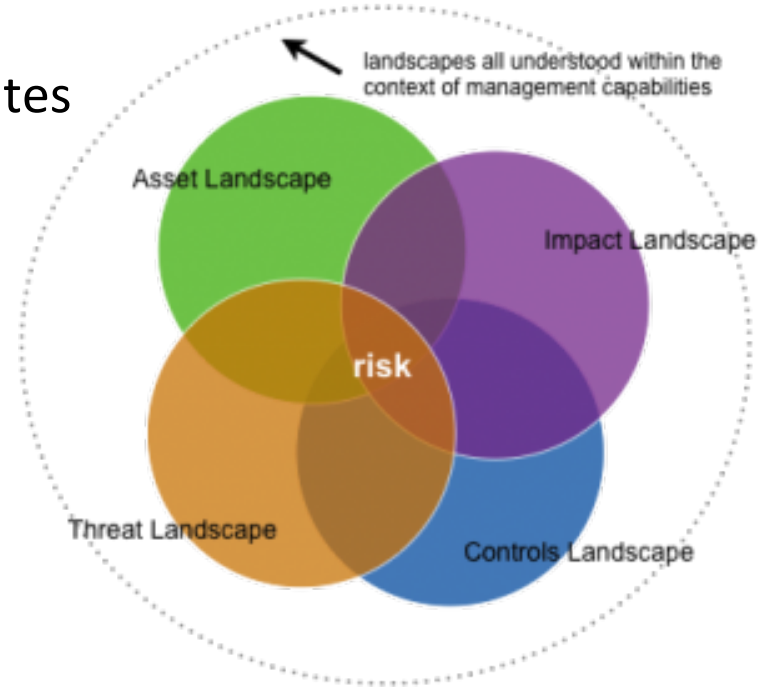
Historical Cyber Incident Data (Free)

- Privacy Rights Clearinghouse: 10,325,490,449 records breached from 8,092 breaches since 2005. Chronology of Data Breaches as a source of info to assist in research involving reported data breaches.
- VERIS Community Database: Vocabulary for Event Recording and Incident Sharing. An open and free repository of publicly-reported security incidents in VERIS format. 7833 Records, 2397 fields per record (90% of fields are empty).
- HHS OCR Wall of Shame: 262,274,896 individuals affected in 2,287 breaches. Required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals.
- Ponemon Institute Research: Cost of a Data Breach Study. 10 Years of non-scientific survey data. Includes a clear statement of limitations.
- Chubb's Cyber Risk Index℠: 556,254,033 insureds' exposed records in past 20 years. Data provided as percentages within categories or ranges.

CYBER RISK DATA SOURCES

VERIS SCHEMA - Structured Data
Actors, Actions, Assets and Attributes

- Incident Tracking
- Victim Demographics
- Incident Description
- Discovery & Response
- Impact Assessment



CYBER RISK DATA SOURCES

PONEMEON COST OF A DATA BREACH

Part 5. Limitations

Our study utilizes a confidential and proprietary benchmark method that has been successfully deployed in earlier research. However, there are inherent limitations with this benchmark research that need to be carefully considered before drawing conclusions from findings.

- **Non-statistical results**: Our study draws upon a representative, non-statistical sample of global entities experiencing a breach involving the loss or theft of customer or consumer records during the past 12 months. Statistical inferences, margins of error and confidence intervals cannot be applied to these data given that our sampling methods are not scientific.
- **Non-response**: The current findings are based on a small representative sample of benchmarks. In this global study, 419 companies completed the benchmark process. Nonresponse bias was not tested so it is possible that companies that did not participate are substantially different in terms of underlying data breach cost.

CYBER RISK DATA SOURCES

PONEMEON COST OF A DATA BREACH

Part 5. Limitations

- **Sampling-frame bias**: Because our sampling frame is judgmental, the quality of results is influenced by the degree to which the frame is representative of the population of companies being studied. It is our belief that the current sampling frame is biased toward companies with more mature privacy or information security programs.
- **Company-specific information**: The benchmark information is sensitive and confidential. Thus, the current instrument does not capture company-identifying information. It also allows individuals to use categorical response variables to disclose demographic information about the company and industry category.
- **Unmeasured factors**: To keep the interview script concise and focused, we omitted other important variables from our analyses such as leading trends and organizational characteristics. The extent to which omitted variables might explain benchmark results cannot be determined.

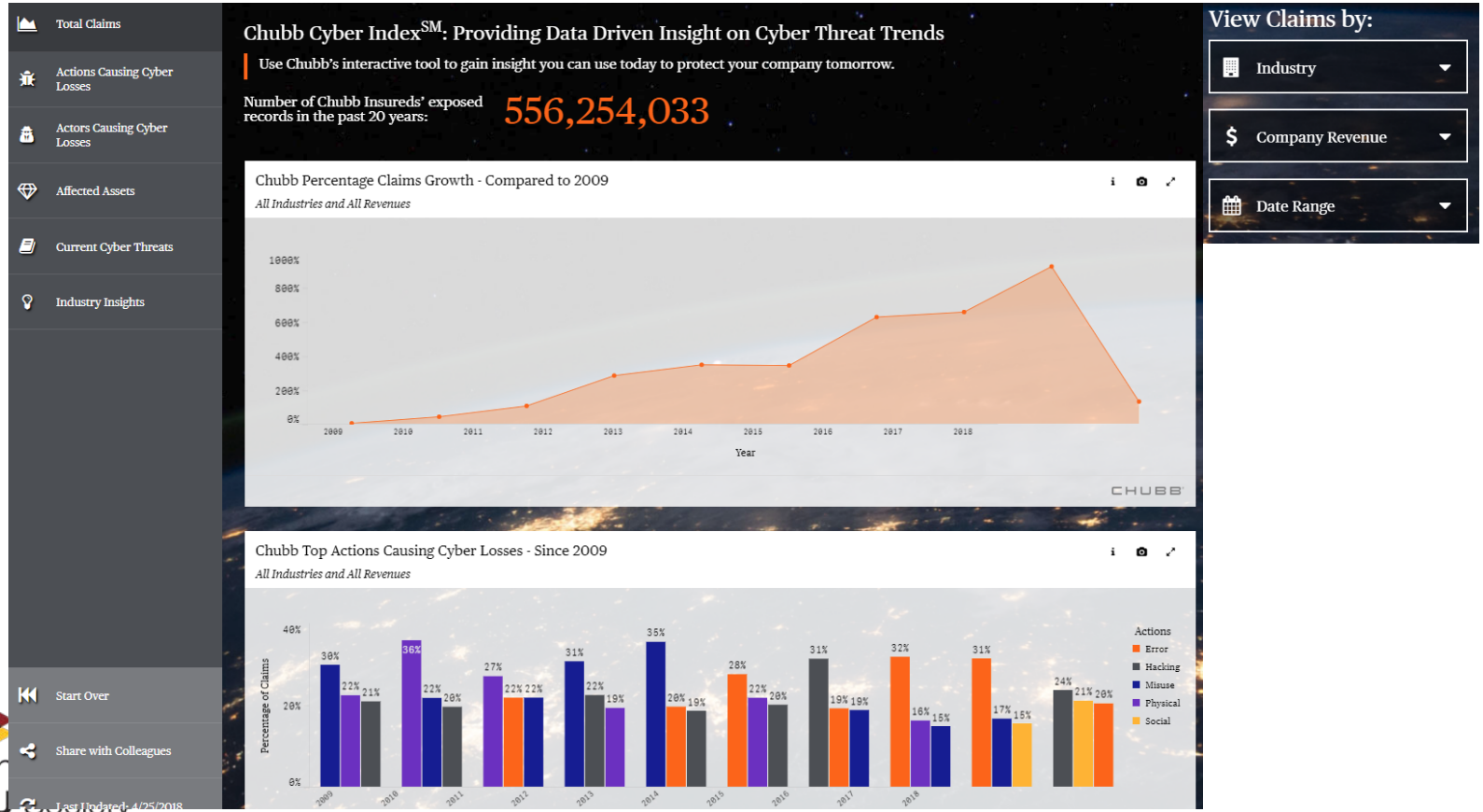
CYBER RISK DATA SOURCES

PONEMEON COST OF A DATA BREACH

Part 5. Limitations

- **Extrapolated cost results**: The quality of benchmark research is based on the integrity of confidential responses provided by respondents in participating companies. While certain checks and balances can be incorporated into the benchmark process, it is always possible that respondents did not provide accurate or truthful responses. In addition, the use of cost extrapolation methods rather than actual cost data may inadvertently introduce bias and inaccuracies.
- **Currency translation gains and losses**: This year**,** a strong U.S. dollar significantly influenced the global cost analysis. The conversion from local currencies to the U.S. dollar deflated the per capita and average total cost estimates, especially for companies in the U.K., Germany, France and Italy (e.g., the Pound (£) and Euro (€)). For purposes of consistency with prior years, we decided to continue to use the same accounting method rather than adjust the cost. It is important to note, that this issue only affects the global analysis because all country-level results are shown in local currencies.

CYBER RISK DATA SOURCES



CYBER RISK DATA SOURCES

Historical Cyber Incident Data (Not free)

- Advisen Cyber Loss Data: 55,000 cyber events "curated by professionals with a wealth of insurance industry expertise." Smaller fraction include loss data.
- NetDiligence Cyber Claims Study: (Free and paid versions) 10 years of reports. Includes analysis of loss data. Small sample sizes. Much improved in the last 2 years.

CYBER RISK DATA SOURCES

Historical Cyber Incident Data Challenges

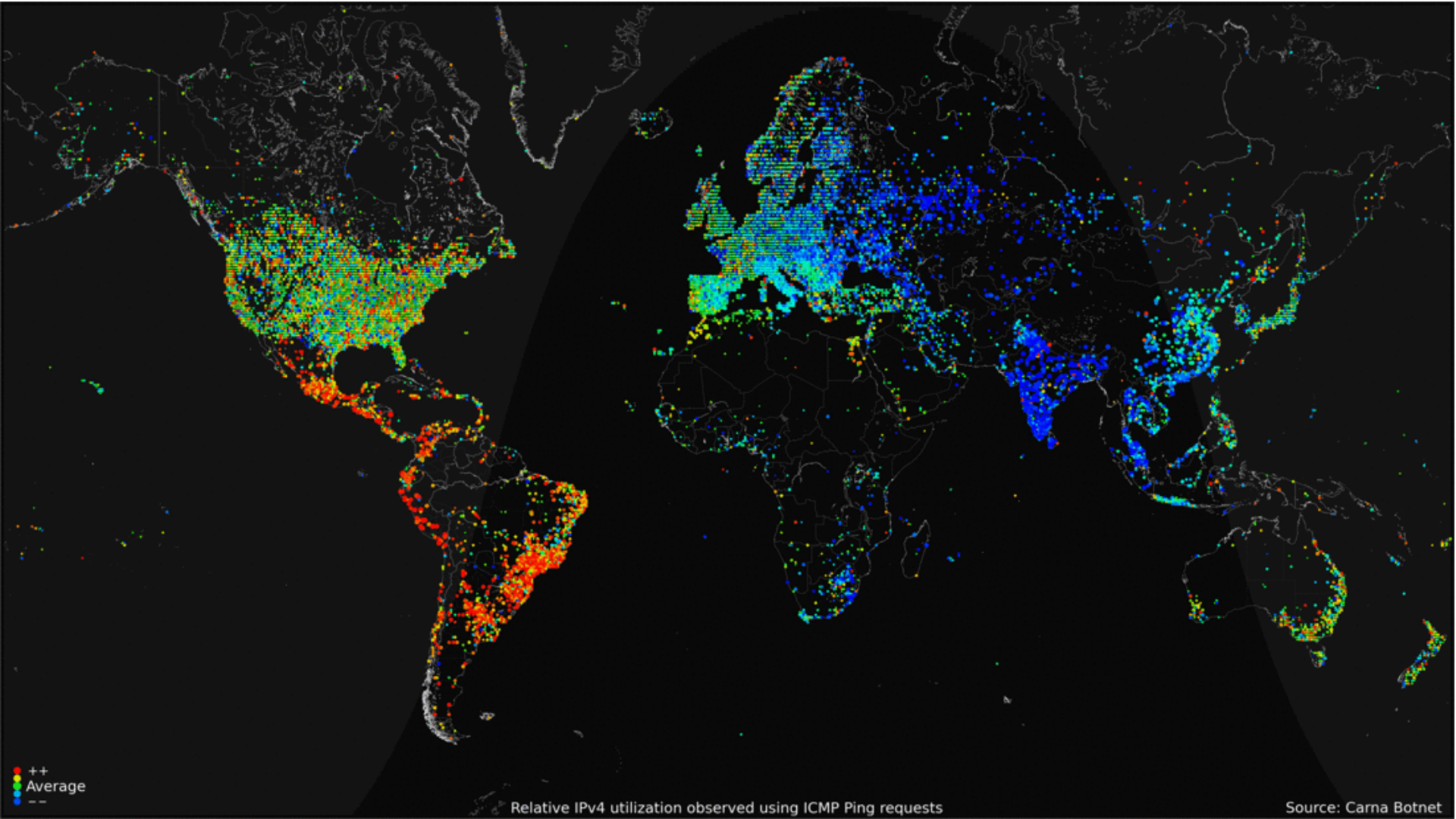
- Data Quality Issues
  - "20-50% of cyber risk data obsolete annually" – Cyber Underwriter
  - Completeness – general lack of loss data, cause of loss, other details
  - Appropriateness: Causes of cyber loss change rapidly
    - Obsolete
    - Lag time between incident occurrence and discovery/reporting
- Sampling methods and bias

OUTSIDE-IN CYBER DATA

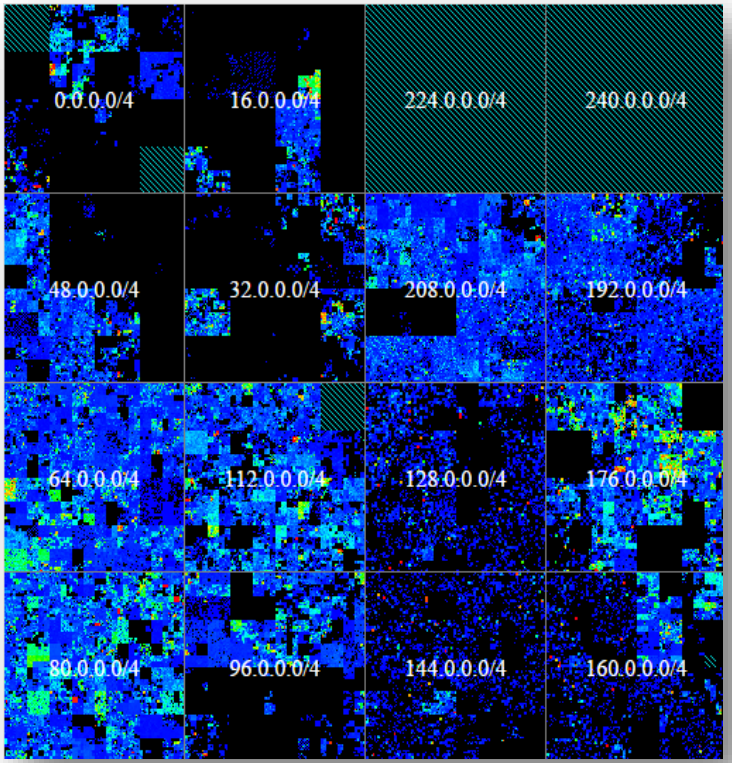
OUTSIDE-IN CYBER DATA

What is "Outside-In" Cyber Data?

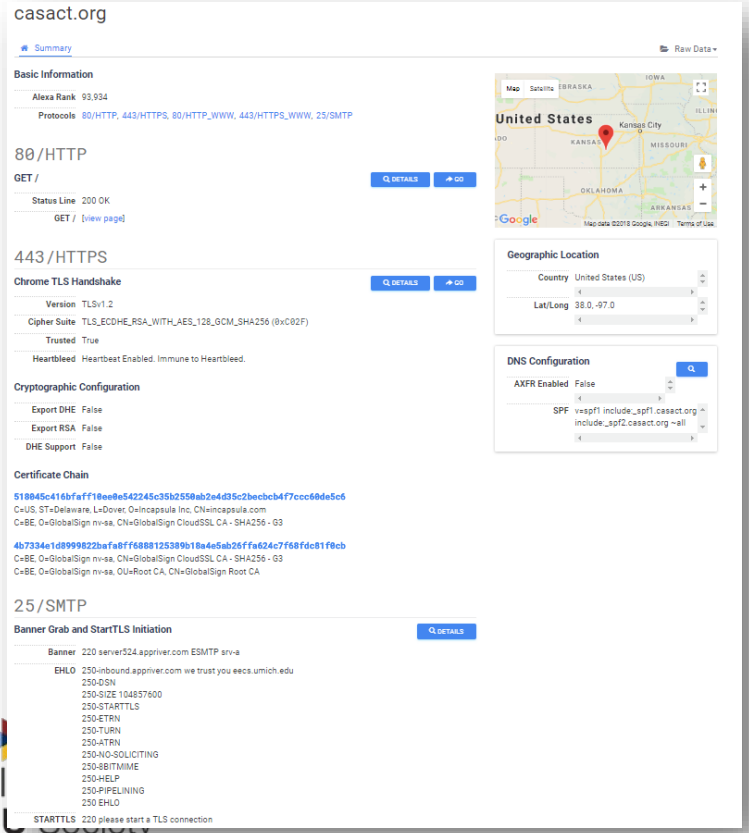
- Uses current, externally observable, non-intrusive data collection
  - Scanning & crawling
- Thousands of data points for each single risk
- Combined with other data sources
- And secret sauce…

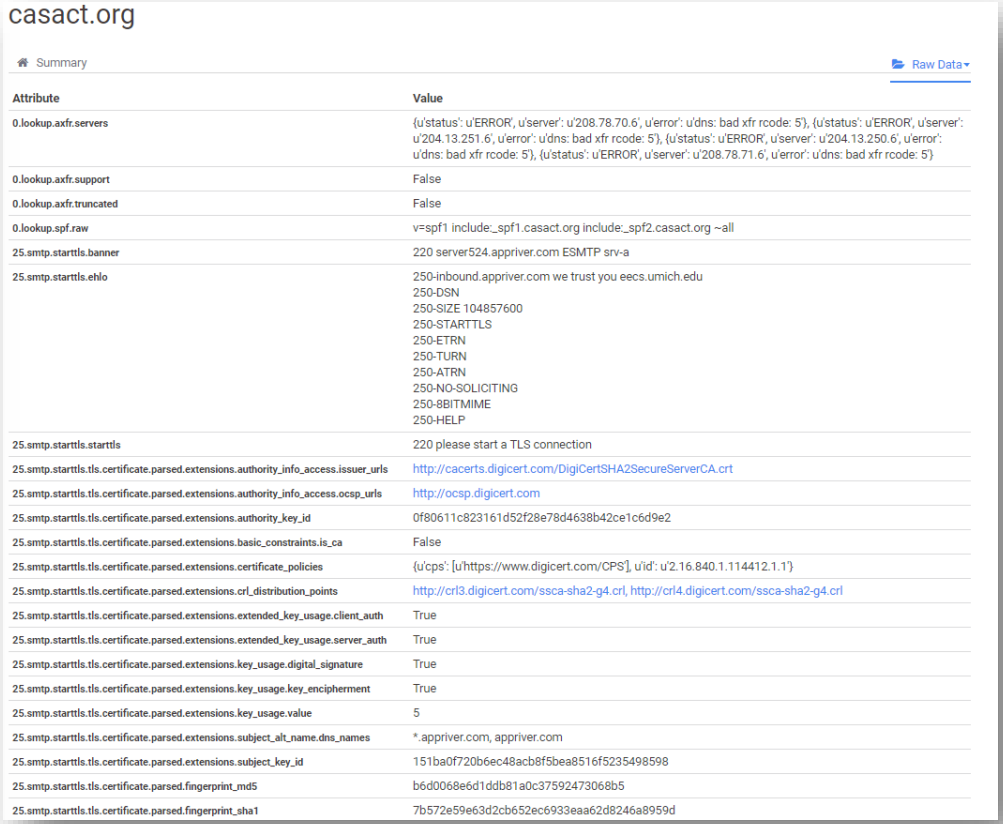

++
Average
--
Relative IPv4 utilization observed using ICMP Ping requests
Source: Carna Botnet

OUTSIDE-IN CYBER DATA



OUTSIDE-IN CYBER DATA





OUTSIDE-IN CYBER DATA

[redacted].131

Summary | WHOIS | Raw Data

Basic Information

OS	Win32
Network	[redacted]
Routing	[redacted].0/23 via AS7018, AS174, AS40177
Protocols	443/HTTPS, 80/HTTP

80/HTTP

GET / DETAILS GO

Server	Apache httpd 2.2.22
Status Line	500 Internal Server Error
Page Title	500 Internal Server Error
GET /	[view page]

Geographic Location

Country	United States (US)
Lat/Long	38.0, -97.0

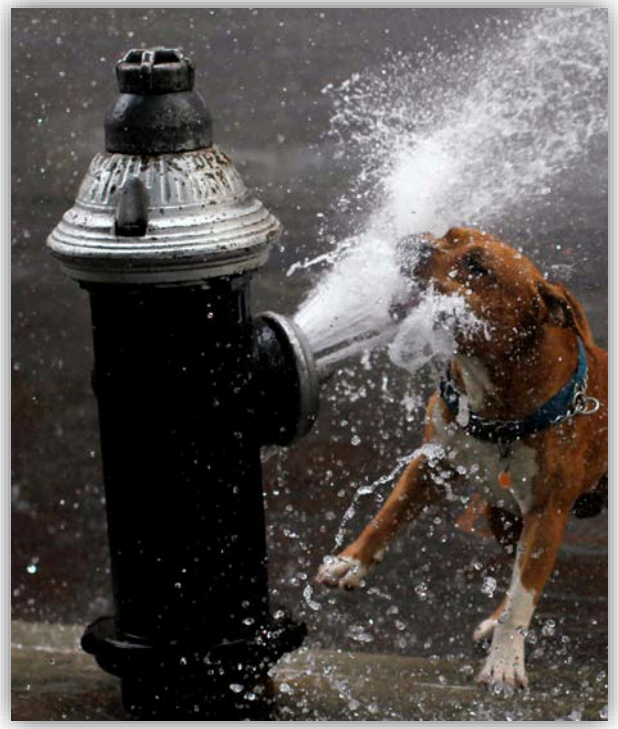
443/HTTPS

Chrome TLS Handshake DETAILS GO

Version	TLSv1.2
Cipher Suite	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
Trusted	True
Heartbleed	Heartbeat Enabled. Immune to Heartbleed.

Cryptographic Configuration

SSLv3 Support	True ⚠ This host is vulnerable to the POODLE attack.
Export DHE	False
Export RSA	False
DHE Support	True



The In
CPCU Society

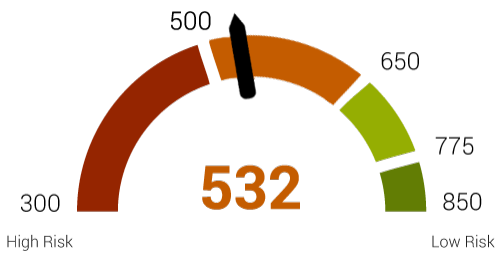
OUTSIDE-IN CYBER DATA

"Outside In" assessment of "security risk posture"

- FICO Enterprise Security Score 300-850
- Security Scorecard - Grade A-F
- BitSight Security Score 250-900

OUTSIDE-IN CYBER DATA

- FICO*:
  - Predictive - “Forecasts the likelihood of a future material data breach.”
  - Empirical - “Machine learning models that utilize historical data breach patterns.”



*http://www.fico.com/en/products/fico-enterprise-security-score

OUTSIDE-IN CYBER DATA

- BitSight*:
  - Security Rating Platform generates “quantitative measurements” of security performance
  - Daily security ratings ranging from 250 to 900
  - Analyzes existing security incidents and practices to produce these ratings
  - “Better than subjective questionnaires and self-assessments”
  - 12 months of historical data and comparisons with industry benchmarks

*https://www.bitsighttech.com/security-ratings-cyber-insurance

OUTSIDE-IN CYBER DATA

- Security Scorecard*:
  - Similar “Outside-In” assessment technique
  - Continuously monitor the security posture of vendors and business partners in a policyholder’s ecosystem

*https://securityscorecard.com/solutions/cyber-insurance

OUTSIDE-IN CYBER DATA

- Outside-In Data Challenges
  - How predictive is scan data?
  - Transparency of scores?
  - Limitations not clearly stated (base rate?)
  - Loss data?
  - Correlation across risk factors?
  - False positives?
  - Utilization of historical cyber data?

INSIDE-OUT CYBER DATA

INSIDE-OUT CYBER DATA

What is “Inside-Out” Cyber Data?

- Cyber Insurance Application
- Cyber Security Audit Information
- Cyber Telemetry Data (Internal System Generated Data)

INSIDE-OUT CYBER DATA

Insurance Applications

- Incomplete
  - Interdependent Security: Cloud and other third party resources play an increasing role in IT and represent greater portion of the cyber risk
- Unreliable
  - Interpretations of technical questions may vary
  - Knowledge may be incomplete or inaccurate
  - Security infrastructure may vary across an organization
  - IT and Security infrastructure changing rapidly

INSIDE-OUT CYBER DATA

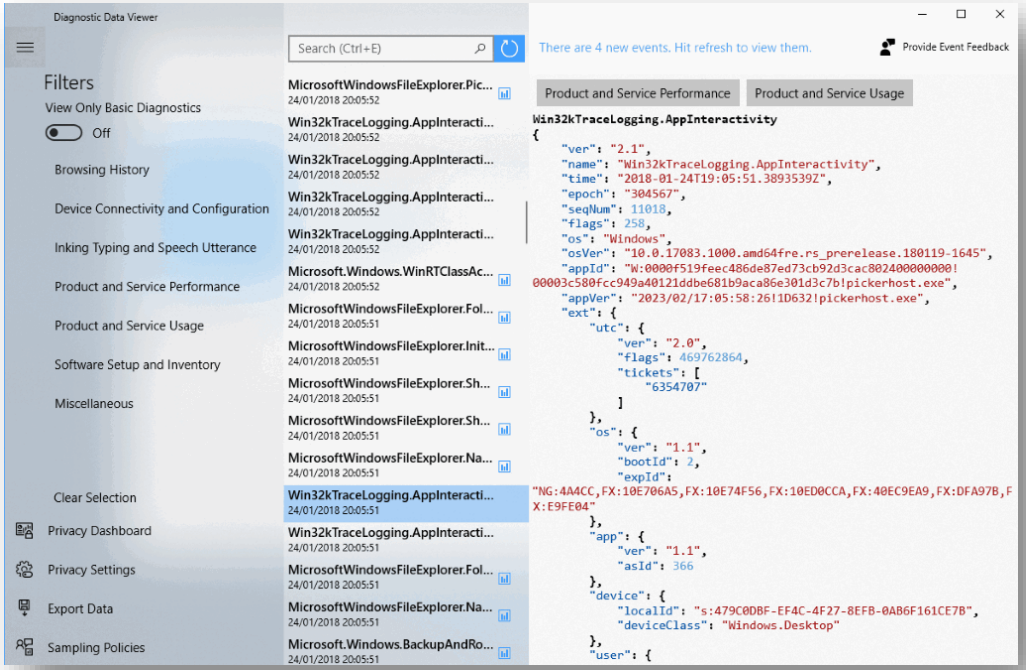
Internal Cyber Risk Assessment

- Comprehensive, including non-technical controls
- Slow and relatively expensive
- Multiple frameworks, inconsistent data
- General lack of quantitative foundation
  - "Control catalogs are codification of infosec folklore, with the caveat that some folk remedies do work." – Infosec Quant
- Frequency of audits
- Audited security controls are frequently subject to risk propagation

INSIDE-OUT CYBER DATA

Cyber Telemetry Data - Internal System Generated Data

- Currently collected by Cisco, Microsoft, Google, Apple, security vendors, etc.
- Potential privacy obligations



INSIDE-OUT CYBER DATA

Cyber Telemetry Data - Internal System Generated Data

- CyRisk*
  - Provides pseudonymized analysis of telemetry data
  - Accurate view of actual enterprise activity
  - Provides pseudonymized telemetry data that supports silent cyber risk analysis
  - Provides aggregated telemetry data that supports cyber accumulation risk analysis

*https://cyrisk.com

INSIDE-OUT CYBER DATA

Cyber Telemetry Data Challenges

- Telemetry data is passive, near real-time
- Relies on expert interpretation
- Not widely available to insurers
- Can detect current risks but predictive value?
- Loss data?
- Correlation across risk factors?

CYBER DATA & AGGREGATION RISK

4A Security & Compliance

CYBER DATA & AGGREGATION RISK

- Risk propagation
- Interdependent security
- Network effect & IT monoculture

RISK PROPAGATION

CYBER DATA & AGGREGATION RISK

Risk propagation

- WannaCry Attack - 230,000 computers in more than 150 counties*
- NotPetya Worm (not ransomware) - Spread from Ukrainian accounting software
  - A.P. Moller-Maersk $200-300M
  - Saint-Gobain €330M
  - Mondelez International net revenues down 5%
  - Merck & Co. $300M
  - FedEx $310M

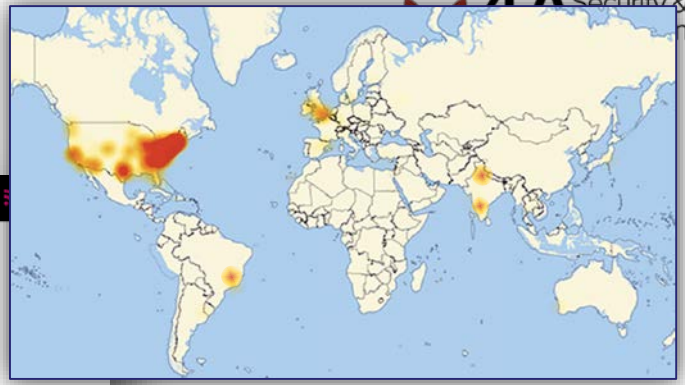
*Council of Insurance Agents & Brokers https://www.ciab.com/resources/cyber-risk-aggregation/

INTERDEPENDENT SECURITY

SECTIONS HOME SEARCH The New York Times

TECHNOLOGY

Hackers Used New Weapons to Disrupt Major Websites Across U.S.



THE VERGE TECH SCIENCE CULTURE CARS REVIEWS LONGFORM VIDEO MORE

REPORT / TECH / CYBERSECURITY

The internet apocalypse map hides the major vulnerability that created it

Where's the infrastructure?

by Ingrid Burrington | Oct 24, 2016, 10:10am EDT

SECTIONS SEARCH Chicago Tribune SUBSCRIBE LOG IN

TUESDAY NOV. 15, 2016 BREAKING SPORTS TRENDING OPINION SUBURBS ENTERTAINMENT BUSINESS ADVERTISING 43°

Blue Sky Innovation / Blue Sky Originals

Another internet outage takes down services in U.S. and U.K.

SECTIONS SEARCH Los Angeles Times SUBSCRIBE

TUESDAY NOV. 15, 2016 MOST POPULAR LOCAL SPORTS ENTERTAINMENT POLITICS ORANGE COUNTY OPINION PLACE AN AD

Opinion / Editorial

Editorial The massive U.S. Internet outage demonstrates the dumb power of smart devices

NBC CT Home News Weather Troubleshooters Entertainment ••• WATCH LIVE TV 46° Connect

Local U.S. & World Decision 2016 Sports Weird Clear the Shelters

3rd Cyberattack 'Has Been Resolved' After Hours of Major Outages: Company

The company at the heart of the attack told CNBC it was hit by "tens of millions of IP addresses" Friday afternoon

GIZMODO SPLOID PALEOFUTURE IO9 SCIENCE REVIEWS FIELD GUIDE

This Is Why Half the Internet Shut Down Today

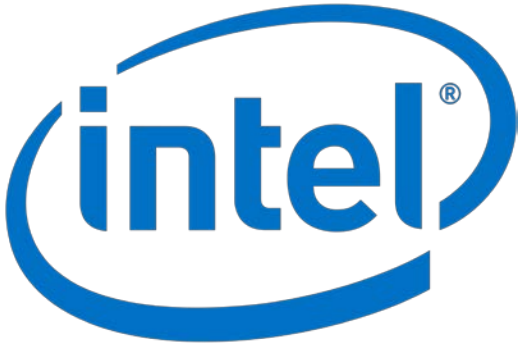
CYBER DATA & AGGREGATION RISK

Interdependent Security - Dyn attack knocked 1,000s of sites offline for a day.

NETWORK EFFECT & IT MONOCULTURE

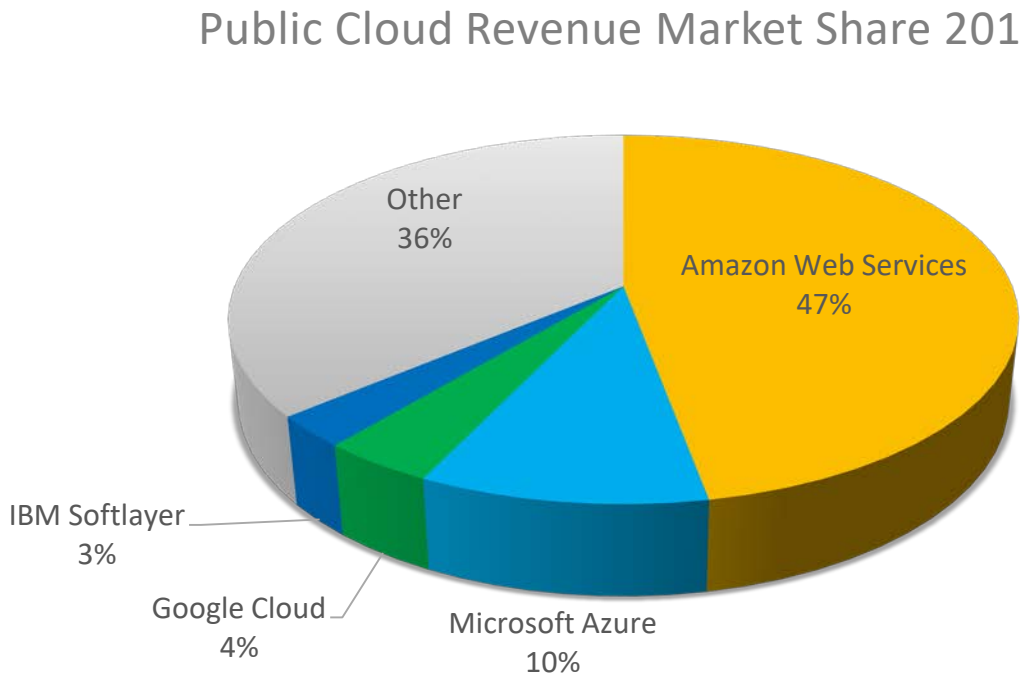
CYBER DATA & AGGREGATION RISK

Network effect & IT monoculture



CYBER DATA & AGGREGATION RISK

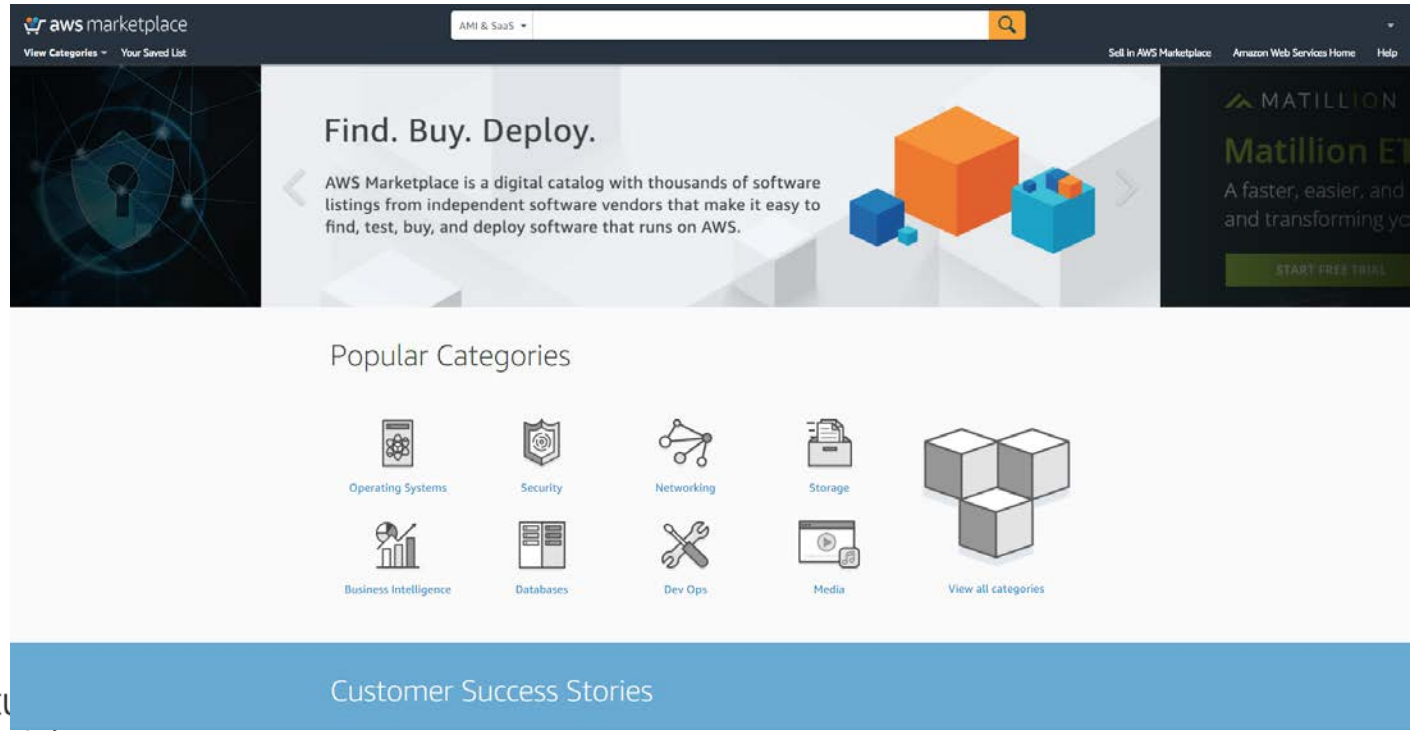
Network effect & IT monoculture



https://www2018.skyhighnetworks.com/cloud-security-blog/microsoft-azure-closes-iaas-adoption-gap-with-amazon-aws/

CYBER DATA & AGGREGATION RISK

Network effect & IT monoculture



CYBER DATA & AGGREGATION RISK

Network effect & IT monoculture

Amazon S3 Outage

Impact on Top 100 Websites

CYBER DATA & AGGREGATION RISK

- New sources of cyber data can be used to provide detailed view of cyber risk aggregation
- Of particular importance for reinsurers since market share analysis can be far off from actual population

CYBER RISK DATA
FINAL NOTES

4A Security & Compliance

CYBER RISK DATA

Cyber Risk Data Sources

- Historical Data – quality issues, incomplete, quickly out-of-date
- Automated Data Sources “Outside In” & “Inside-Out”
- Still work to do testing predictive value
- More transparency needed on Cyber Scores
- Promising opportunity to address cyber risk aggregation

AUDIENCE POLL

Audience Poll

Are you now more likely to break out Cyber from other coverages in analysis:

1. Yes
2. No
3. N/A

Audience Poll

Are you now more/less likely to purchase historical cyber data?

1. More
2. Less
3. Same
4. N/A

Audience Poll

Are you now more/less likely to purchase "Outside In" Cyber Data?

1. More
2. Less
3. Same
4. N/A

Audience Poll

Are you now more/less likely to purchase "Inside Out" Cyber Data?

1. More
2. Less
3. Same
4. N/A

Audience Poll

Are you now more or less confident in your pricing & underwriting?

1. More
2. Less
3. Same
4. N/A

Audience Poll

Are you more/less likely, if asked, to recommend aggressively growing this book:

1. More
2. Less
3. Same
4. N/A

THANK YOU!

QUESTIONS?

Ben Goodman, Founder & CEO

4A Security & Compliance

goodmanb@4asecurity.com

484-858-0427

Michael Solomon

FCAS, MAAA, CERA

MichaelSolomon613@gmail.com

The Actuarial Advantage, Inc.

TAA