Cyber Risk and Public Policy: The American Academy of Actuaries Assesses Cyber Risk

Steve Jackson, Ph.D.

Director of Research (Public Policy)

American Academy of Actuaries

CREAR International Workshop on Cyber Risk & Security September 13–14, 2023

Agenda

1. American Academy of Actuaries—Background
2. Academy Research:
   a. Cyber Breach Reporting Requirements
   b. Cyber Risk Toolkit
   c. Modeling Cyber Risk with Data which does not specify Dollar Losses
3. Conclusion

American Academy of Actuaries—Background

History of the American Academy of Actuaries

In the 1960s, there were four major actuarial organizations in the United States. With increasing reliance in federal legislation on actuarial opinions, there was a clear need for a single actuarial association focused on public policy issues and professionalism that would represent all US actuaries.

- 1965: The Academy was established by the original four organizations
- Today: The Academy has >19,500 members / ~30,000 actuaries in U.S.*
- Mission: Serve the public and the U.S. actuarial profession

* Source: U.S. Department of Labor, Occupational Outlook Handbook

Public Policy Activities

- Comment letters
- Issue briefs
- Practice notes
- Actuarial analysis for specific public policy bodies
- Systematic research

Research

Until 2016, research by volunteers primarily involved reliance on literature or proprietary research by companies

- Exceptions: Life insurance experience studies and Actuaries Longevity Illustrator (in partnership with the Society of Actuaries), Casualty risk-based capital reports to National Association of Insurance Commissioners.

In 2016, a director for research was hired to guide the creation of a research program, working with both volunteers and staff.

In 2017, cyber risk identified as one of the first areas of focus.

Research on Cyber Risk

NOVEMBER 2020

CYBER BREACH REPORTING REQUIREMENTS

AN ANALYSIS OF LAWS ACROSS THE UNITED STATES

American Academy of Actuaries
Cyber Risk Task Force, Casualty Practice Council

American Academy of Actuaries
Objective. Independent. Effective.™

ACTUARY.ORG

Cyber Breach Reporting Requirements: 2020

- No uniform national standards exist for notifying consumers and authorities of data breaches
- Each state and territory has its own statute(s) with notification requirements
- In July 2018, a U.S. Department of the Treasury report concluded:
  - Differences in state laws can make compliance overly burdensome for companies doing business in more than one state
  - U.S. Congress should enact data security and breach notification legislation that applies uniform standards across the states

Findings

Scope: All cover PII of state residents.

Covered Information: All states use name in tandem with one other trigger. Twenty-three states only have 3-4 triggers, while the rest vary between 5 and 15.

Form of Covered Information: All include electronic records. Only six include written records.

Breach Definition: “Unauthorized” or “illegal” access; good-faith exceptions in all but three jurisdictions.

Findings (cont'd)

Safe Harbor/Exceptions: In every jurisdiction for encrypted data.

Harm Threshold: All but 14 states only require notification if some level of harm is likely.

Consumer Notice: Notice required as soon as possible. Only 15 states stipulate deadline, ranging between 30 and 90 days. Substitute notice available in 50 of 54 jurisdictions for varying cost thresholds.

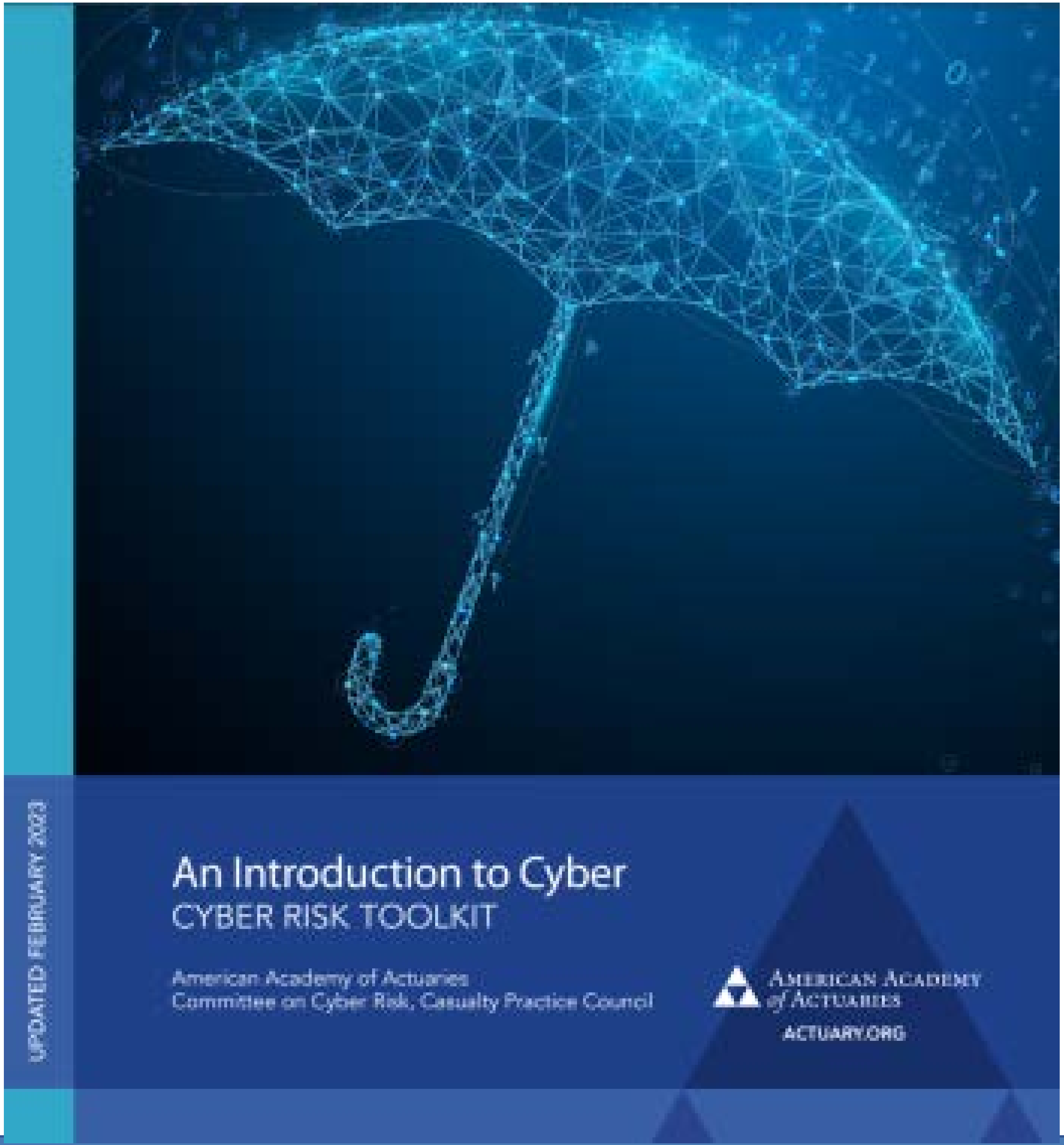
Government Notice: Only 36 states explicitly require notification to authorities.

Findings (cont'd)

Consumer Reporting Agency (CRA) Notice: Often required if certain number of consumers are affected, ranging from 500 to 10,000 with a median threshold of 1,000.

Third-Party Notice: Data owner must be notified immediately in all but two states.

Potential Penalties: Civil penalties may be imposed for violation in all cases.



UPDATED FEBRUARY 2023

An Introduction to Cyber

CYBER RISK TOOLKIT

American Academy of Actuaries
Committee on Cyber Risk, Casualty Practice Council

AMERICAN ACADEMY
of ACTUARIES
ACTUARY.ORG

Cyber Risk Toolkit

- Developed and maintained by the Academy’s Cyber Risk Task Force, now Committee on Cyber Risk
- Intended to be a resource for interested readers of the general public, public policymakers, the actuarial profession, the insurance sector, and other stakeholders
- While each is a standalone paper, in total they offer a cohesive overview of the challenges posed in the cyber insurance market
- The toolkit will continue to be updated periodically to reflect new and emerging work from the committee

Cyber Risk Toolkit: Contents

- An Introduction to Cyber
- Cyber Threat Landscape
- Silent Cyber
- Cyber Data
- Cyber Risk Accumulation
- Cyber Risk Reinsurance Issues
- Ransomware
- War, Cyberterrorism, and Cyber Insurance
- Autonomous Vehicles and Cyber Risk
- Digital Assets and Their Current Roles Within Cybercrime
- Cyber Risk Resource Guide

Upcoming:

Vendor Models
Cryptocurrency & Cyber Risk
Personal Lines Cyber Risk & Insurance

Academy Collaboration With Professor Kratz

A. Applying to U.S. data the methodology developed for the Gendermarie Nationale cyber data including the algorithm by Dacorogna, Debbabi, and Kratz (2023) to assess the extremes

B. Objectives:
- Produce robust estimates for cyber risk in the U.S.
- Examine changes in risk over time, across categories
- Compare results to comparable French results

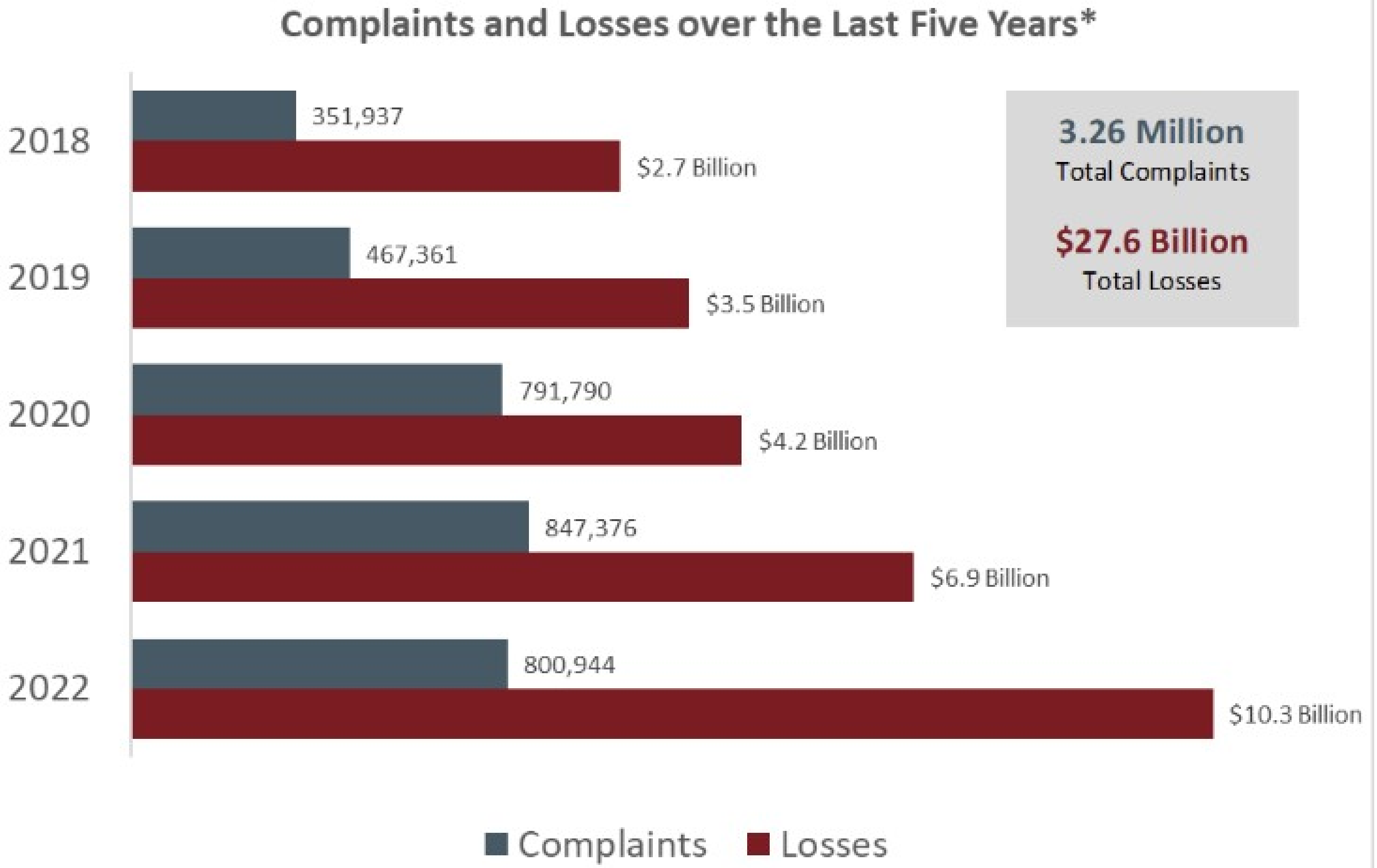
C. A project in two phases:
- Phase 2 is the goal
- Phase 1 is a pilot project to facilitate Phase 2

A Project in Two Phases: Phase 2

Target Database:

- FBI's Internet Crime Complaint Center (IC3) Database
- IC3 began receiving complaints in 2000
- In 2022, received ~800,000 complaints
- In 2022, $10.3 billion in losses reported
- Since 2000, more than 7M complaints
- Since 2000, more than $35B in losses
- Access to IC3 requires demonstration to FBI of intended use

Source: Federal Bureau of Investigation, Internet Crime Report 2022



A Project in Two Phases: Phase 1

Phase 1 Database:

- Identity Theft Resource Center (ITRC) Database of breaches of personally identifiable information (similar but superior to Privacy Rights Clearinghouse database)
- Academy has licensed data from 2009 to 2021
- In 2021, ITRC documents 2,410 breaches (1,311 with number of people impacted), with 2.1 billion individuals' records impacted
- Between 2009 and 2021, 14,114 breaches (8,002 with number of people impacted), with 11.5 billion individuals' records impacted
- Analysis completed in fall 2023 (expected)

Issue of Converting People Impacted Into Losses

ITRC (and PRC) do not report losses. They do report “People Impacted” or “Records Breached” or both.

Some analysts simply look at numbers of people/records.

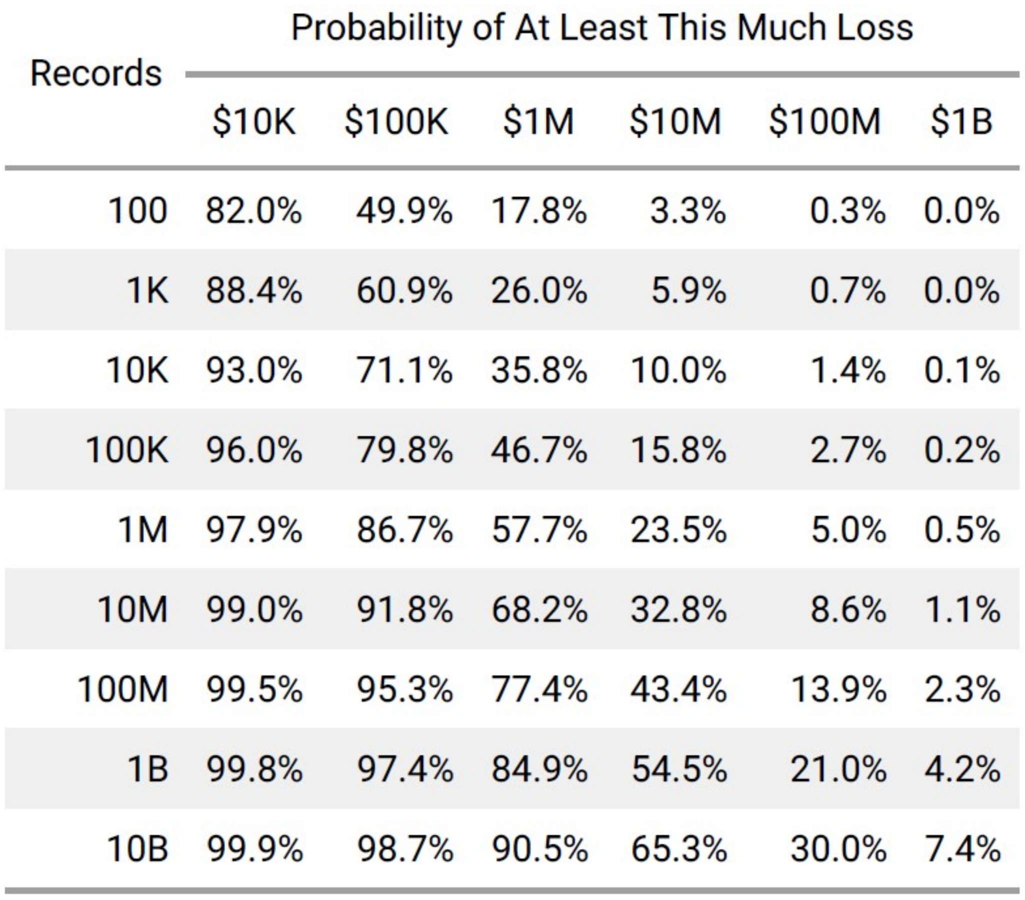
Many convert numbers of people/records into losses by one of two methods:

- IBM Annual Cost of a Cyber Breach Data Report, with estimate of $ per record (e.g. 2021: $161)
- Jacobs (2014): Ln(Loss) = 7.68 + 0.76*Ln(Records)

Issue of Converting People Impacted Into Losses

- Jacobs (2014): “After looking at this data, I would caution anyone using these models to take them all with a grain of salt. While using something like the log-log model above may be able to provide a frame of reference where there is currently a lot of uncertainty, the amount of variance in the model is a serious challenge to adoption.”
- Cybersecurity and Infrastructure Security Agency (2020): “Cyentia (2020) provides the most illustrative explanation of how severe the variability in the cost-per-record metric has been in historical data and the resulting pitfalls of relying on the direct scaling of per-record estimates.”
- Cyentia (2020): “We hope this exposes the folly (and puts the last nail in the coffin) of loss estimates based on a simple average cost per record derived from a limited range of data.”

Issue of Converting People Impacted Into Losses



Records	Probability of At Least This Much Loss					
	$10K	$100K	$1M	$10M	$100M	$1B
100	82.0%	49.9%	17.8%	3.3%	0.3%	0.0%
1K	88.4%	60.9%	26.0%	5.9%	0.7%	0.0%
10K	93.0%	71.1%	35.8%	10.0%	1.4%	0.1%
100K	96.0%	79.8%	46.7%	15.8%	2.7%	0.2%
1M	97.9%	86.7%	57.7%	23.5%	5.0%	0.5%
10M	99.0%	91.8%	68.2%	32.8%	8.6%	1.1%
100M	99.5%	95.3%	77.4%	43.4%	13.9%	2.3%
1B	99.8%	97.4%	84.9%	54.5%	21.0%	4.2%
10B	99.9%	98.7%	90.5%	65.3%	30.0%	7.4%

Table 4: Probable losses based on records affected in a breach

Cyentia (2020):

"Table 4 should help those wanting to estimate losses based on the number of records affected by a cyber event. a breach of 100K records will almost certainly (96% chance) cost at least $10K but probably won't (2.7% chance) exceed $100M. Not as easy as multiplying by $150, but it'll go a long way toward better risk assessments."

Issue of Converting People Impacted Into Losses

RATIO of ESTIMATES to PUBLISHED VALUE	Cyentia Mean of Bounds	Cyentia, Mean of Logs of Bounds	Cyentia Lower Bound	Cyentia Upper Bound	Jacobs (2014)
ALL (15)					
Mean	415.17%	**270.70%**	**137.08%**	693.26%	**5294.43%**
Median	**81.09%**	55.72%	24.56%	**129.93%**	**1494.37%**
SENSITIVE (8)					
Mean	648.94%	**421.31%**	**210.78%**	1087.11%	**5206.99%**
Median	167.76%	**113.88%**	58.91%	271.47%	**3086.36%**
>= 100M people impacted (7)					
Mean	**63.52%**	43.93%	25.80%	**101.25%**	**5578.74%**
Median	57.48%	39.09%	22.08%	**92.88%**	**1494.37%**

Conclusion

Academy research is assisting the public, policymakers, and actuaries understand cyber risk better.

Current research (Phase 2) should provide much better estimates of cyber risk in U.S. than presently available.

Current research (Phase 1) is adding to the understanding of data limitations and ways in which to respond, for both academic and non-academic analysts.

Sources Not Already Described

1. U.S. Department of the Treasury (July 2018). A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation.
2. Michel Dacorogna, Nehla Debbabi. and Marie Kratz (2023). Building up cyber resilience by better grasping cyber risk via a new algorithm for modelling heavy-tailed data. European Journal of Operational Research, 311.
3. Jay Jacobs (2014). Analyzing Ponemon Cost of Data Breach. Posted on R-Bloggers.com, December 11, 2014.
4. Cybersecurity and Infrastructure Security Agency [CISA] (2020). Cost Of A Cyber Incident: Systematic Review And Cross-validation. October 26, 2020.
5. Cyentia Institute (2020). Information Risk Insights Study: A Clearer Vision for Assessing the Risk of Cyber Incidents.

Questions or comments:

Contact Steve Jackson
Director of Research (Public Policy)
American Academy of Actuaries
sjackson@actuary.org