Cyber Risk and Financial Stability – An Atlas for Macroprudential Analysis

Project on Cyber Risk to Financial Stability

Columbia University's School of International and Public Affairs

Rachel Adeney, Jason Healey, Patricia Mosser, Danielle Waiss

Disclaimer

The co-authors are affiliated with Columbia University's School of International and Public Affairs. This paper are their own views and do not necessarily reflect those of any affiliated organization.

Overview

- Part of a 5+ year effort at SIPA

- Goal: provide a guide to data/information currently available to assess cyber risks to financial stability
  - High level summary of data sources and potential research uses
  - Assessment of currently available data and information
  - What's missing?

Cybersecurity Data Groupings
Relevant for Financial Stability Analysis

- Systemic risk analysis of cyber risks have been plagued by a lack of relevant data
- Macroprudential policymakers and researchers seem to rely on a smaller set of data than used by cybersecurity practitioners and researcher
- This paper is perhaps the first major categorization (not a taxonomy) of relevant cybersecurity data
  - Still draft and incomplete
  - Still gaps to be filled

Pioneering Researchers Are Using Some of these Data

Our Categorization May Help Further

- Data on losses from specific cyber incidents can be used to understand the nature and consequences of cyber risks over time
  - Aldasoro et al (2020) 'Operational and cyber risks in the financial sector'
  - Palsson et al (2020) 'Analysis of the impact of cyber events for cyber insurance'
  - Bouveret (2018) 'Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment'
  - Romanosky (2016) 'Examining the costs and causes of cyber incidents'
  - Cope et al (2012) 'Macroeconomic determinants of operational loss severity'
- Cyber ratings and other data on preparedness can be used for risk assessments
  - Kaffenberger and Kopp (2019) 'Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment'

How Can the Data Inform Our Research Questions?

Research Questions
How vulnerable are financial institutions to cyber incidents?
How are the adversaries actually targeting financial institutions (or might they in different geopolitical circumstances)?
What is the impact of cyber incidents on financial institutions?

How Can the Data Inform Our Research Questions?

Research Questions	Data
How vulnerable are financial institutions to cyber incidents?	Cyber ratings data, spending on IT and cybersecurity, surveys of resilience and outcomes, public macro data
How are the adversaries actually targeting financial institutions (or might they in different geopolitical circumstances)?	Media reports, intelligence and cybersecurity reports, cybersecurity databases, databases of pooled information
What is the impact of cyber incidents on financial institutions?	Cyber loss data available in media and survey reports, mandatory reporting, commercial databases, restricted databases

Many Different Ways to Categorize Data Sources

Three Important Slices

- Research Topic
  - Protection and preparedness
  - Threat assessment and intelligence
  - Economic and business impact

Many Different Ways to Categorize Data Sources

Three Important Slices

- Research Topic
  - Protection and preparedness
  - Threat assessment and intelligence
  - Economic and business impact
- Source and Availability
  - Based on unit of analysis and where the data are generally found
  - Restricted, Commercial, Open-Source (Public)

Many Different Ways to Categorize Data Sources

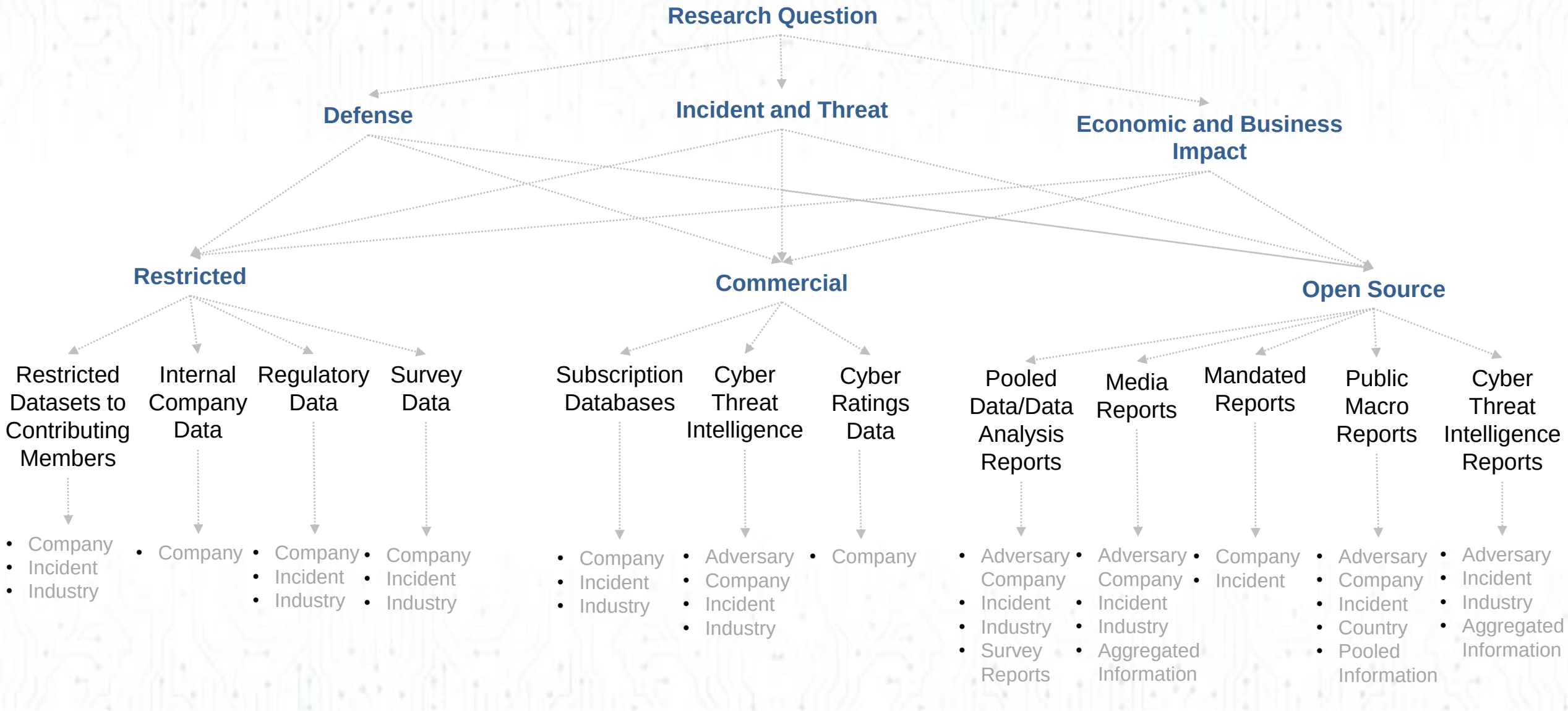
Three Important Slices

- Research Topic
  - Protection and preparedness
  - Threat assessment and intelligence
  - Economic and business impact
- Source and Availability
  - Based on unit of analysis and where the data are generally found
  - Restricted, Commercial, Open-Source (Public)
- Data Types
  - How are the data presented and level of effort necessary to conduct independent quantitative analysis
  - Raw data, existing database, pooled information, reports

Research Topic

- **Defense**
  - Data on firms' preparedness for cyber incidents includes a host of indicators that help an entity understand their degree of vulnerability to cyber threats.
  - Includes a number of metrics like ratings on firms' cyber security and practices, investment and spending on cyber security, and country-level data on IT access
  - Endogenous to defenders
- **Incident and Threat**
  - **Incident-based data** are those collected, usually from sensors on an affected computer or network or intermediate points (such as by an Internet Service Provider). It does not rely on knowing which threat actor was involved, though it can help determine that.
  - **Threat intelligence data** are those collected and analyzed to provide insight on a threat actor's motivations, targets and behaviors to understand what they have done in the past, help anticipate what they might do next and implement appropriate countermeasures.
  - Exogenous to defenders
- **Economic and Business Impact**
  - Inform the cost/benefit analysis of cyber security investments by individual firms, particularly as it relates to investment in controls. This information helps policymakers understand the magnitude of the impact of a cyber incidents and where they occur so they can assess the potential implications for financial stability.

Data Source Map



Data Source Table

		Research Topic		
		Defense	**Incident and Threat**	**Economic and Business Impact**
Availability of data	**Restricted**		- Collective data on cyber incidents - Individual data on cyber incidents	- Cyber loss data
	Commercial	- Cyber ratings - Spending on cyber security	- Cyber threat intelligence data	- Cyber loss data
	Open Source	- Reports on cyber security spending and practices - IT access, use and investment across countries	- Cyber threat intelligence data - Cyber threat intelligence reports - Media reports	- Mandated reporting on incidents - Reports on incidents

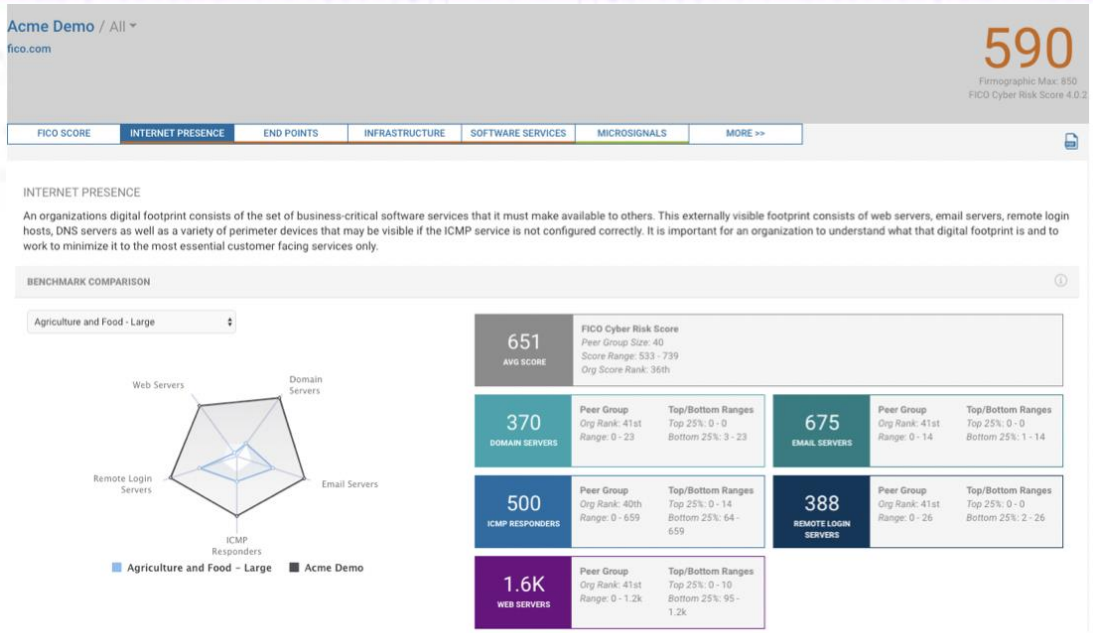
CYBER PROTECTION AND PREPAREDNESS

How vulnerable are we?

Cyber Ratings

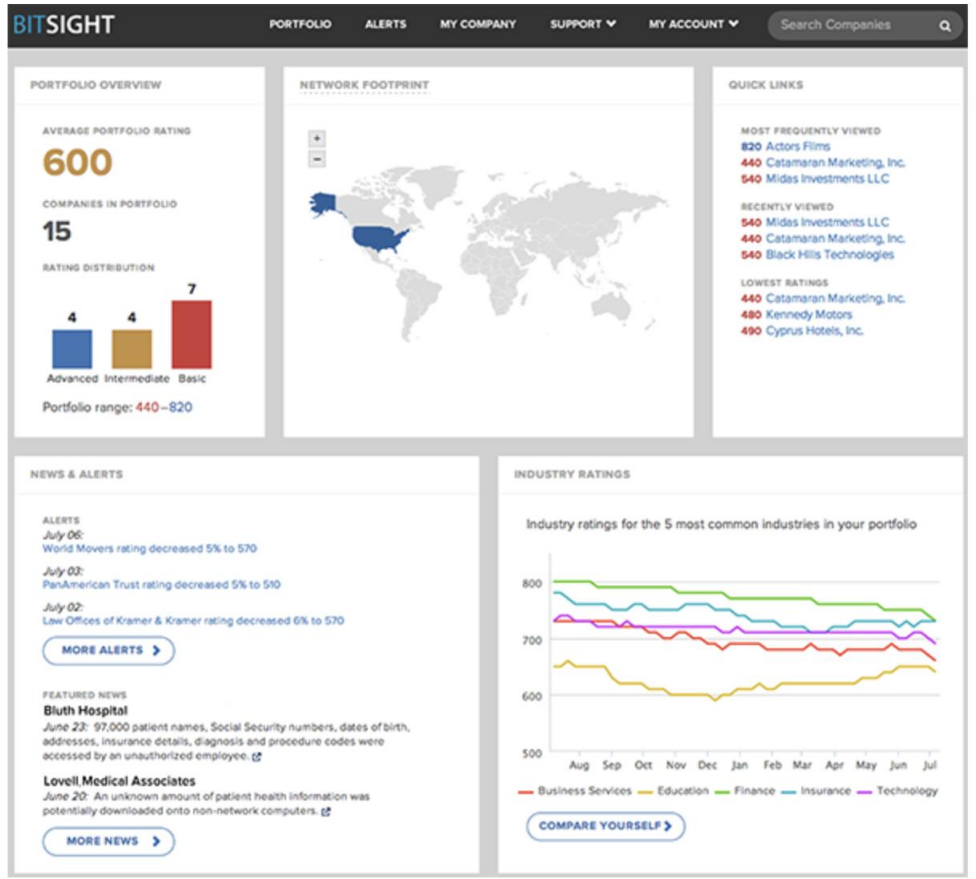
- Ratings data use standardized methodology based on a large set of externally observable factors
  - Can include technical factors like computers involved in a botnet and organizational factors like board members who understand security)
  - Not publicly available, usually requiring a subscription for each company
  - Unit of analysis is a single company
- Rating is presented as cybersecurity "risk scores" (like the US FICO) for commercial purposes:
  - Assess risk at a single company (primary purpose)
  - Evaluate supply chain risk (as compilation of individual ratings)
  - Assess risk in an entire sector
  - Track risk migration over time
  - Inform M&A activity
  - Guide insurance underwriting
- **Bitsight, Security Scorecard, and FICO Cyber Risk Score** are contenders in this space
  - For example, Bitsight found that companies with the lowest scores are 5 times more likely to suffer a cyber incident than those with the highest
- Research Uses: Compare security between companies, track over time, examine sectors and supply chain, compare cyber with credit risk
- Drawbacks: difficult to get the data on enough companies to use in thorough quantitative analysis

Cyber Ratings



FICO Cyber Risk Score

RiskRecon



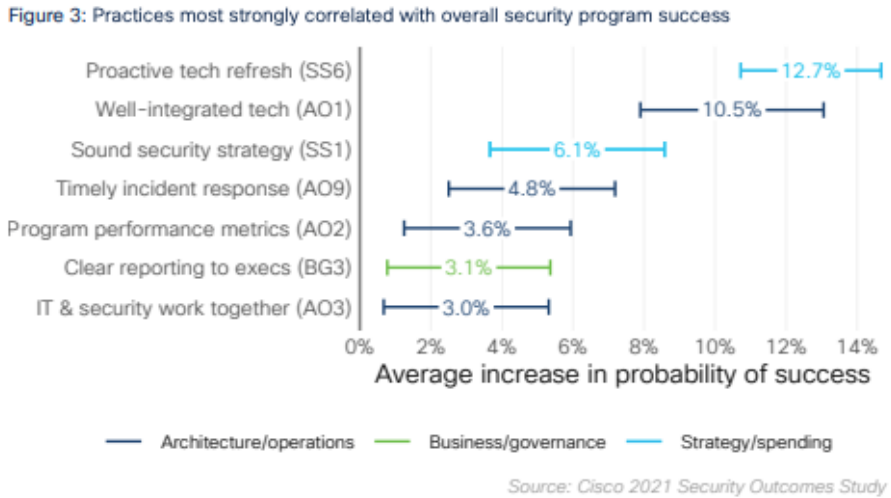
Bitsight

Cybersecurity and IT Spend

- Firms' investment in IT and cybersecurity can indicate their preparedness for adverse cyber events
- Research uses:
  - How has IT/cyber spend changed alongside increased cyber risks and adverse events
  - How has spending on particular security measures changed
  - How effective is this spending (difficult to assess)
- Examples:
  - **Gartner Forecast Analysis**: Information Security, Worldwide
    - Forecasts of IT spending
  - **IDC Worldwide Security Spending Guide**
    - Five-year forecasts of security spending for 47 countries, 20 industries and multiple technology groups, published semi-annually

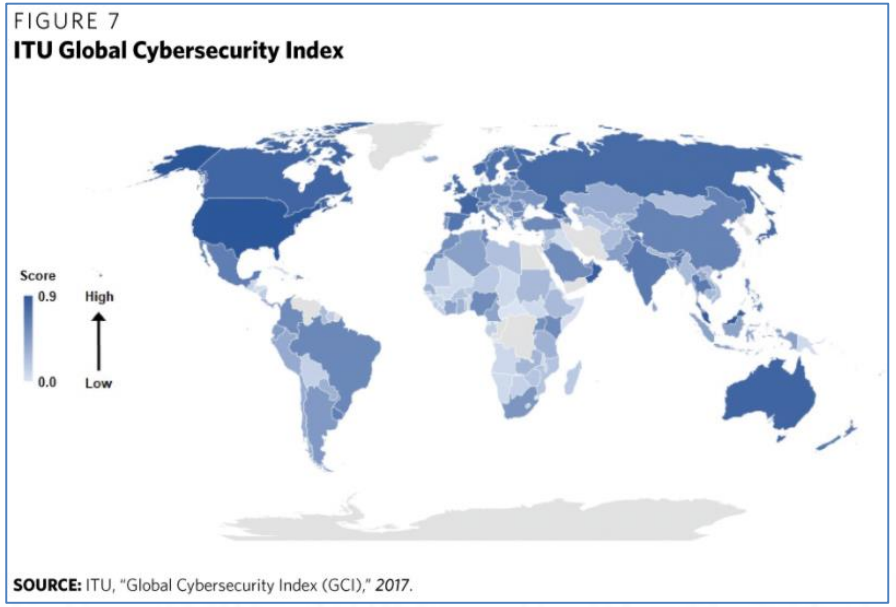
Surveys

- **Cisco/Cyentia Institute 2021 Security Outcomes Survey**
  - Survey about adherence to security practices and their level of success
- **SANS 2020 IT Cybersecurity Spending Survey**
  - Includes data on spending trends for the use of public cloud infrastructure, spending on new threats, spending for emerging privacy/security legislation, spending on the security workforce and the effectiveness of security spending
- **2020 IIF/McKinsey Cyber Resilience Survey**
  - Financial services industry survey about firm and sector level cyber resilience, adequacy of spending on cybersecurity
- **PwC's Global State of Information Security**
  - Annual survey of over 9,500 C-suite level individuals over the past 20 years
- **Index of Cybersecurity**
  - Sentiment-based measure of perceived risk and has climbed almost every month since its creation in 2011
- Research Uses: Surveys help our understanding of sentiment, state of security in individual organizations
- Drawbacks: many surveys are one-offs



Public Macro Data

- Publicly available data on IT access, use, and investment across countries.
  - Examples: World Bank Global Findex Database, ITU Global Cybersecurity Index, OECD ICT Access and Usage by Businesses
  - Research uses: cross country comparisons of the reliance on technology and vulnerability to cyber attacks
  - Drawbacks: highly aggregated; mixed availability of data across countries and time



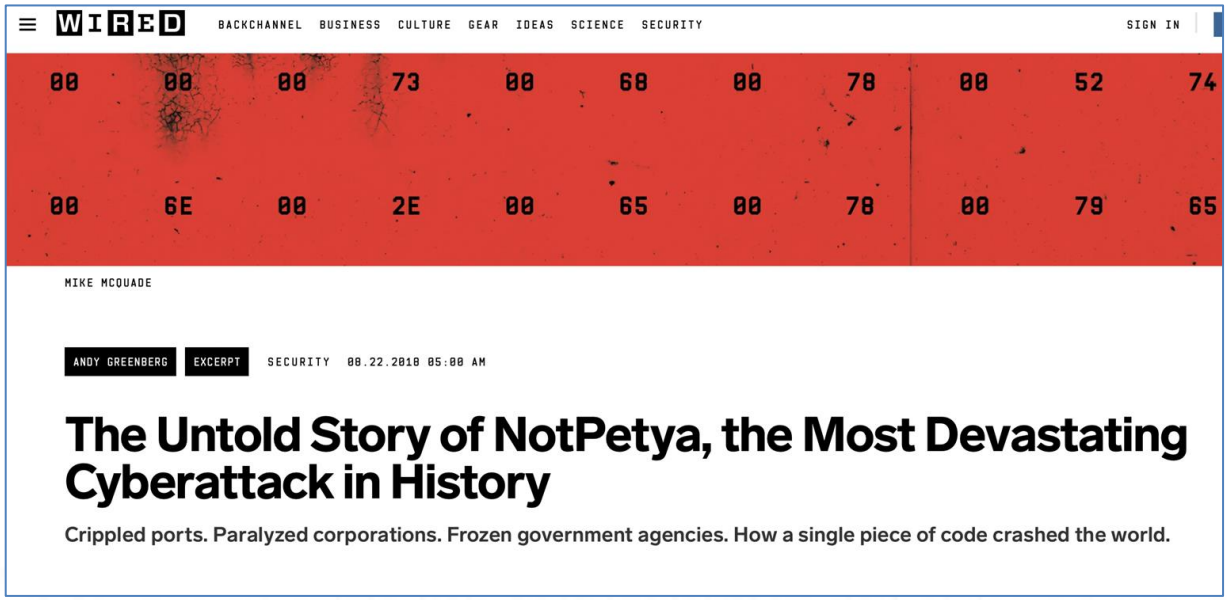
CYBER THREAT ASSESSMENT AND INTELLIGENCE

What are the adversaries doing?

Media Reports

- Means by which the public regularly learns of breaches and incidents.
- Several journalists are specifically focused on these topics.
  - Brian Krebs routinely breaks news about intrusions
  - These reports can include information on insurance payout information.
    - Andy Greenberg at Wired extensively covered the impact of NotPetya

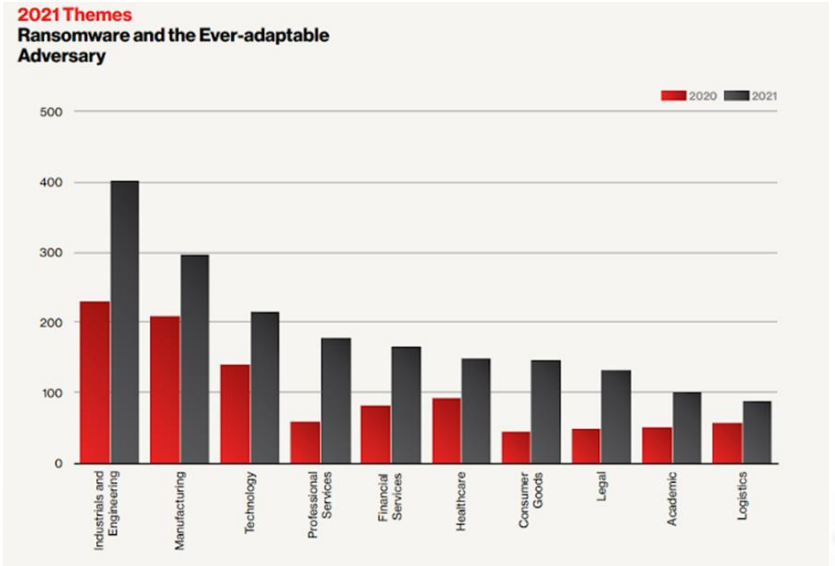
- Research use: event analysis, track incidents by geography, create dataset on attack details from information reported, NLP analysis.
- Drawbacks: Larger effort to collect data for any quantitative analysis. Data is limited to what is covered by the media.



Intelligence and Cybersecurity Reports

- Threat intelligence companies and cybersecurity vendors issue annual or quarterly intelligence reports with useful information
  - **Intelligence reports** focus predominantly on each threat actor (criminals or a nation, like China, Russia, or Iran)
  - **Cybersecurity reports** focus on detected attacks, such as the largest denial-of-service attacks and the trends
  - Often will include information by industry under attack, like North Korea targeting the global payments network
  - Essentially marketing for the companies: reports do not include the full, proprietary data sets

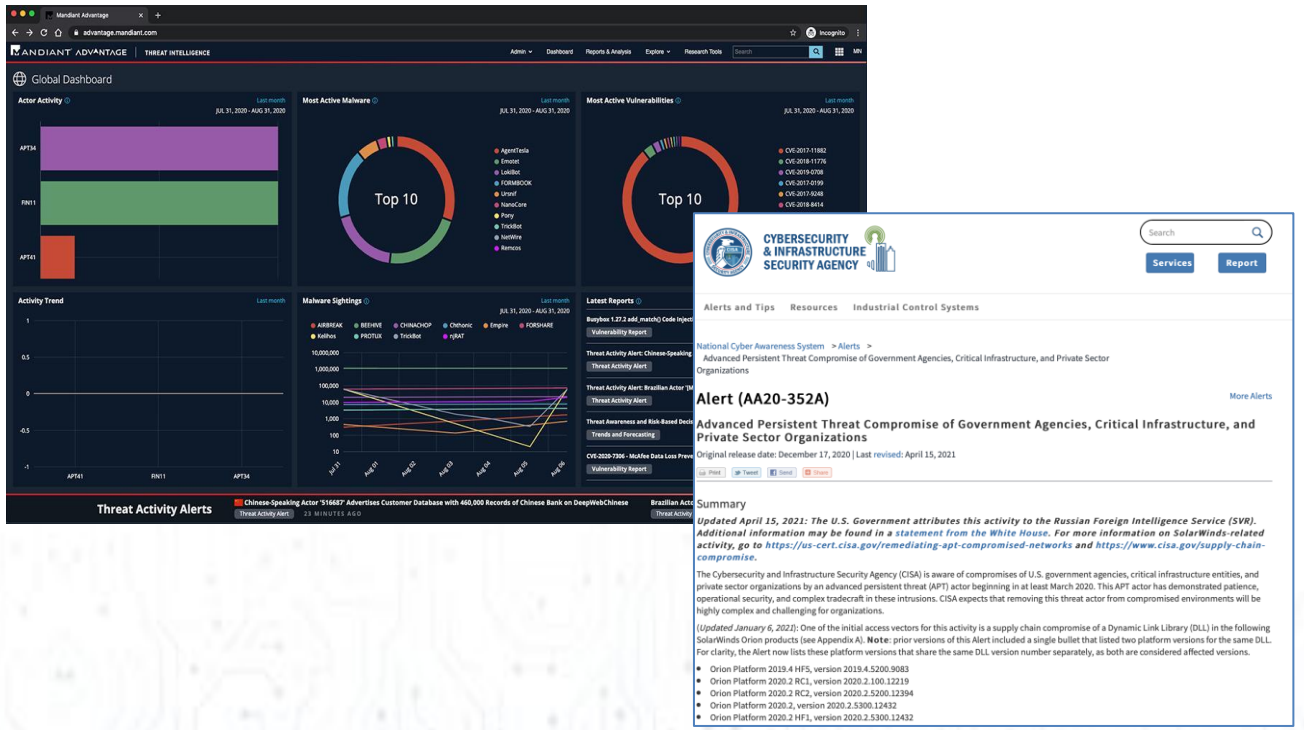
- Examples: Annual threat reports by **Crowdstrike, FireEye, Akamai, Arbor Networks**
- Unit of analysis is a particular adversary (threat intel) or type of infrastructure (vendors)
- Research Uses: Excellent to give view of summary view and trends over time
- Drawbacks: Trends covered may range by publication, limiting analysis across time. Raw data is usually not publicly available.



Technical Cyber Threat Intelligence (CTI)

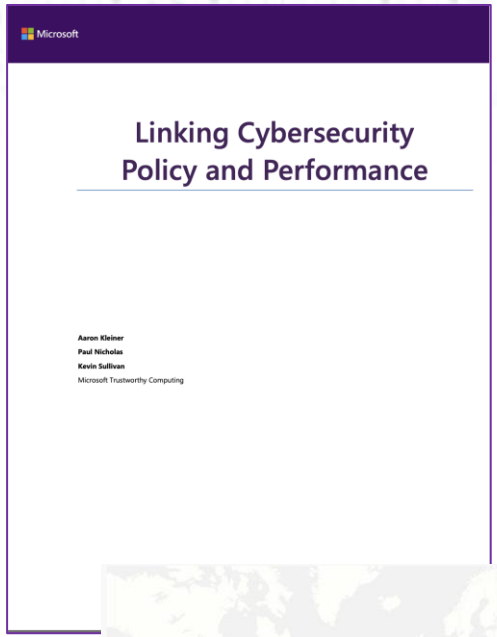
- Technical reports or databases with information highly relevant to cyber defenders including Indicators of Compromise.
- Public CTI: released by government agencies on ongoing threats (openly accessible)
  - DHS, CISA, FBI notices or alerts, CVE database
- Private: Issued by private companies (commercial)
  - Crowdstrike, FireEye CTI

- Research Uses: Useful in examining trends at an adversary or infrastructure level
- Drawbacks: May be too technical and lack the context necessary for economic analysis, unless creatively combined with other data sets.



Harder Datasets on Cybersecurity and Cyber Conflict

- Unit of analysis is usually a specific incident or campaign
- Technical incident-level data (proprietary data)
  - Most fruitful are compiled by those with vast sensor networks or large-scale sharing
  - Examples: Google, Microsoft, Komodo, Cyber Threat Alliance, FS-ISAC
  - And derivative works like Microsoft, “Linking Cybersecurity Policy and Performance” (2013)
  - Others derived from data at individual companies
- Who is attacking whom, with national-security frame (academic-open source)
  - Valeriano, Maness, Jensen; CFR Cyber Operations Tracker



Databases of Pooled Information

- Unit of analysis is usually a specific incident

- **Verizon Data Breach Investigations Report** is the longest and largest dataset, having been running for a decade. Covers thousands of incidents across industry sectors
  - The dataset is downloadable and fully searchable
  - VDBIR sorts by industry sector, nation, kind of incident, and the like
- Research Uses: Extensive, especially for VDBIR which provides entire dataset. Surveys help fill in understand of sentiment, state of security in individual organizations

ECONOMIC/FINANCIAL IMPACT

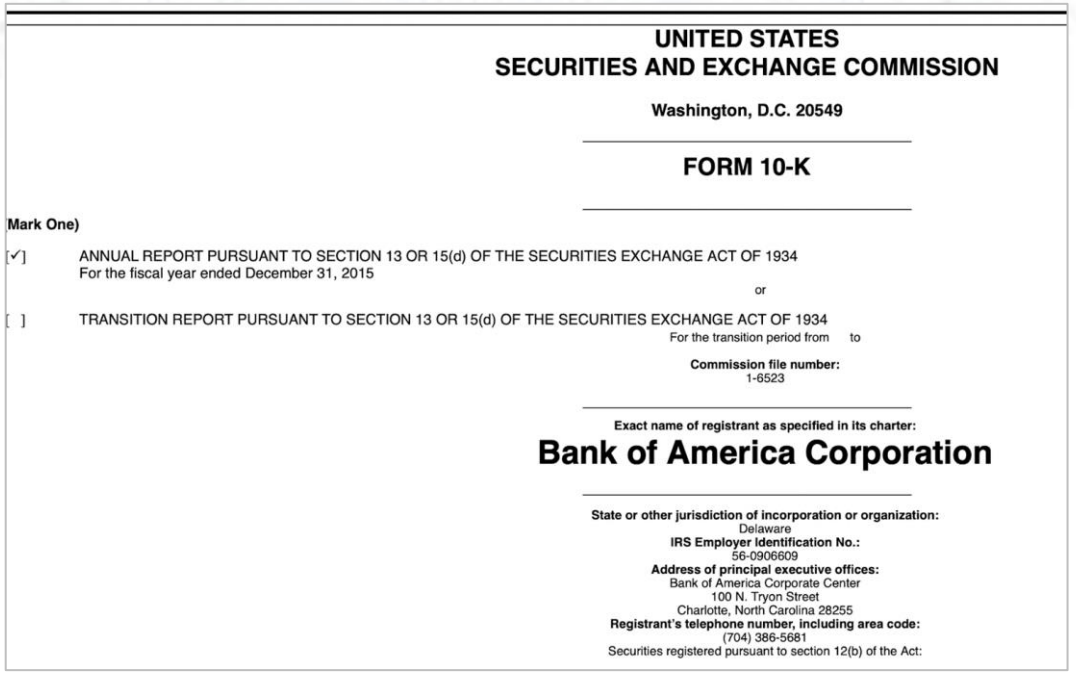
What do we know about the real impacts?

Cyber Losses

- Data on losses from specific cyber incidents
  - Includes media and macroeconomic reports, mandatory company reporting and incident-level databases
  - Sourced from public or private information
  - Publicly available, commercially available or restricted
- Research uses: examine the nature and consequences of cyber events over time
  - Aldasoro et al (2020) 'Operational and cyber risks in the financial sector'
  - Palsson et al (2020) 'Analysis of the impact of cyber events for cyber insurance'
  - Bouveret (2018) 'Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment'
  - Romanosky (2016) 'Examining the costs and causes of cyber incidents'
  - Cope et al (2012) 'Macroeconomic determinants of operational loss severity'

Mandatory Reporting

- Government reporting requirements on financial performance, legal proceedings, reports that are publicly available.
- Unit of analysis is a single company
- Examples from the United States
  - **10K and 10Q reports** submitted to the SEC contain important disclosure information on material risks
  - **FTC findings** including cases, reports, case filings, testimony and public comments
- Research use: measured financial loss (over threshold)in affected companies, track incidents by geography, track governance and board competencies
- Drawbacks: Not databases, difficult to use, reporting lag



UNITED STATES
SECURITIES AND EXCHANGE COMMISSION

Washington, D.C. 20549

FORM 10-K

Mark One)

[✓] ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934
For the fiscal year ended December 31, 2015

or

[ ] TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934
For the transition period from to

Commission file number:
1-6523

Exact name of registrant as specified in its charter:
Bank of America Corporation

State or other jurisdiction of incorporation or organization:
Delaware
IRS Employer Identification No.:
56-0906609
Address of principal executive offices:
Bank of America Corporate Center
100 N. Tryon Street
Charlotte, North Carolina 28255
Registrant's telephone number, including area code:
(704) 386-5681
Securities registered pursuant to section 12(b) of the Act:

US Form 10-K

Commercially Available Databases

- Full databases available for commercial subscription
- Examples:
  - **Advisen Cyber Loss Data**
    - Incident level data built from publicly verifiable sources, covers >90,000 cyber events
    - Includes data on case type and status, affected count, accident date, source of loss, type of loss, loss amount, company characteristics, industry, geography
    - Costs include fines, response costs and legal fees
  - **ORX News**
    - Data on operational risk losses from 2010 onwards, gathered from publicly available information
  - **Netdiligence**
    - Database of cyber loss claims sourced from insurers from 2010
  - **RMS Cyber Loss Experience Database**
    - Incident level database from 2007 covering type of cyber event, geography, firm sector, size and cyber risk attributes (to measure potential losses)
    - Database designed for (re)insurers and incorporates cyber claims data provided by several RMS clients

Restricted Databases

- Databases only available on an anonymized basis to contributing members
  - **ORX Global Loss Data**
    - Database of operational risk losses from 2002 built on data contributed by member banks and insurers
    - Includes data on the number of loss events, loss amounts, losses by business type and geography
    - High level information published annually

Figure 2: Total gross loss of events reported per year

  - **ORX Cyber**
    - Information sharing service for cyber risk management professionals, pilot program launched in 2019
  - **ORIC Loss Database**
    - Database covering over 15,000 operational risk events built on data by contributing members
    - Describes loss events and their causes, loss amounts and geographical data
  - **Verisk Cyber Data Exchange**
    - Database of cyber claims, including losses, claim descriptions, attack vector and source and details of insurance policies
- Other non-public data
  - Internal company data
  - Regulatory reporting
  - Confidential surveys

Reports

- Public reports, but restricted data:
  - **Ponemon Cost of a Data Breach Report** includes details on breach costs across industries and geography, available annually since 2005
  - **One-off reports:** on the impact of cyber on the economy, or sector. Examples:
    - Council of Economic Advisors: "The Cost of Malicious Cyber Activity to the U.S. Economy" (2018)
    - CSIS: "Economic Impact of Cyber Crime" (2018)
    - Atlantic Council: "Beyond Data Breaches: Global Interconnections of Cyber Risk" (2014)
    - Lloyd's: "Business Blackout" on impact of cyberattack on US power grid (2015)
    - Moody's: "Retail and Commercial Banks – Global: Growing digitalization increases banks' cyber risk exposure" (2019, subscription needed)
- Research use: rich information on financial/economic impact
- Drawbacks: Raw data is not available so hard to track evolution of trends or use for quantitative analysis

USES AND LIMITATIONS

How These Data Sources Can Be Used

- Data on losses from specific cyber incidents can be used to understand the nature and consequences of cyber risks over time
  - Aldasoro et al (2020) 'Operational and cyber risks in the financial sector'
  - Palsson et al (2020) 'Analysis of the impact of cyber events for cyber insurance'
  - Bouveret (2018) 'Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment'
  - Romanosky (2016) 'Examining the costs and causes of cyber incidents'
  - Cope et al (2012) 'Macroeconomic determinants of operational loss severity'
- Cyber ratings and other data on preparedness can be used for risk assessments
  - Kaffenberger and Kopp (2019) 'Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment'

Key Data Limitations

- Inability to link various types of data, particularly linking cyber risk indicators to impact data
- Inconsistent (or incompatible) reporting standards
- Outright gaps in data reporting which can result in insufficient sample sizes
- Lack of access

What We Do Not Know (or Can't Measure)

- Incomplete information on system interconnectedness
  - No data on how an incident might be transmitted via both IT and financial systems
  - Require data to map the structure and overlaps of IT interconnections and vendors (e.g. cloud providers) and financial economic interconnections (e.g. counterparty networks)
- Lack of data on IT substitutability (nearly non-existent) and financial substitutability (inadequate)
  - Data on FMIs has improved but they are only one example of a lack of financial substitutability

Q&A