DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof. Reference herein to any social initiative (including but not limited to Diversity, Equity, and Inclusion (DEI); Community Benefits Plans (CBP); Justice 40; etc.) is made by the Author independent of any current requirement by the United States Government and does not constitute or imply endorsement, recommendation, or support by the United States Government or any agency thereof.

SANDIA REPORT
SAND2024-08939
Printed July 2024

Sandia National Laboratories

Sovereign Credit Rating Processes Adapted to Critical Infrastructure Cyber Risk Assessment

Sandia National Laboratories
Kevin Griffith, Asmeret Naugle, Hayden T. Fears, Danielle R. Jacobs, Megan Nyre-Yu, Joshua T. Dise

Zeichner Risk Analytics
Nicholas Winstead, John Arterbury

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico
87185 and Livermore,
California 94550

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology & Engineering Solutions of Sandia, LLC.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: https://classic.ntis.gov/help/order-methods/

ABSTRACT

United States critical infrastructure entities are increasingly targeted by motivated and capable threat actors and must be prepared to assess and treat a diverse range of cyber risks. Consequently, this necessitates some form of analytical process to evaluate risks and inform cyber security investment decisions. A potential solution for structuring cyber risk evaluation exists within the field of sovereign credit ratings – where agencies employ mature approaches that integrate quantitative and qualitative data to produce a singular value of assessment. Adapting such approaches, we present a novel criterion and methodology for measuring and communicating the likelihood element of cyber risk. The methodology is composed of three sequential phases: a quantitative baseline organized by distinct capability frames, a bounded qualitative adjustment per frame, and a greater-bounded qualitative adjustment spanning the entire process. The process culminates in publication of a cyber capability rating that communicates a critical infrastructure entity's ability and willingness to mitigate discontinuous function due to cyberattack.

ACKNOWLEDGEMENTS

We would like to thank Sandia National Laboratories staff members Natalie Prittinen, Jeffrey J. Apolis, Lynn Yang, Ruby E. Booth, and Jason C. Reinhardt for their support and guidance. We would also like to thank several anonymous reviewers for their valuable feedback. This work was supported through contract #70RSAT21KPM000105 with the U.S. Department of Homeland Security Science and Technology Directorate.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

This page left blank

ACRONYMS AND TERMS

Acronym/Term	Definition
AI	Advanced Industrial
BCCR	Baseline Cyber Capability Rating
CCR	Cyber Capability Rating
CEIP	Carnegie Endowment for International Peace
CISA	Cybersecurity and Infrastructure Security Agency
CRA	Credit Rating Agency
CRS	Congressional Research Service
CSIS	Center for Strategic & International Studies
EAD	Exposure at Discontinuity
ECAI	External Credit Assessment Institution
EM	Emerging Markets
ESMA	European Securities and Markets Authority
FCCR	Final Cyber Capability Rating
GAO	Government Accountability Office
GCSCC	Global Cyber Security Capacity Centre
ICCR	Intermediate Cyber Capability Rating
IGD	Impact Given Discontinuity
MAD	Mean Absolute Deviation
NCF	National Critical Function
NIST	National Institute of Standards and Technology
NRSRO	Nationally Recognized Statistical Rating Organization
OLS	Ordinary Least Squares
PD	Probability of Discontinuity
SEC	Securities and Exchange Commission
UN ITU	United Nations International Telecommunication Union
WLC	Weighted Linear Combination

This page left blank

1. INTRODUCTION AND BACKGROUND

Evaluating cyber risk has become increasingly important amidst the prevalence of motivated and capable threat actors targeting critical infrastructure within the United States. Consequences that can be attributed to malicious threat actors include network shutdowns (Center for Strategic & International Studies [CSIS], 2022), nuclear power plant safety monitors disabled (Government Accountability Office [GAO], 2006), and emergency service call center disruptions (GAO, 2005). Such examples represent observed, attributable incidents; but the potential for incidents that yield even greater consequences remains. The pipeline industry offers a concise example. Pipelines have been subject to numerous government cybersecurity alerts (Parfomak & Jaikaran, 2021) regarding threat actor behavior and vulnerabilities. Concurrently, pipelines have exhibiting severe consequences such as environmental damage, destruction of homes, and loss of life (Parfomak, 2012) due to latent control operation dysfunction. Such consequences, though non-intentional, represent possible outcomes that threat actors can attain through access to control systems that are inherent to many critical infrastructure operations. The potential for severe consequences will continue to exist and critical infrastructure entities must be prepared to assess and treat a diverse range of cyber risks. Thus, some form of analytical process to evaluate risk and inform cybersecurity investment decisions is necessary.

A potential solution for structuring cyber risk evaluation exists within the field of sovereign credit ratings – where agencies employ mature approaches that integrate quantitative and qualitative data to produce a singular value of assessment. Sovereign credit ratings have existed since the early 1900's, when seminal agencies Moody's, Poor's Publishing, and Standard Statistics issued their first ratings (Bhatia, 2002). Since then, the market for ratings has expanded to encompass a multitude of issuers authorized by U.S. Securities and Exchange Commission (SEC) as Nationally Recognized Statistical Rating Organizations (NRSRO) or authorized by the European Securities and Markets Authority (ESMA) as Credit Rating Agencies (CRA). Across issuers, the integration of quantitative and qualitative data is a key methodological feature and has been found to generate significantly more accurate default predictions than single use of either data type (Grunert, Norden, & Weber, 2005) and that qualitative data is informative to predicting default over short time horizons (De Moor, Luitel, Sercu, & Vanpée, 2018). Though shortcomings are documented in the form of qualitative bias – positive bias toward home or economically and culturally proximate sovereigns and negative bias toward foreign sovereigns that are economically and culturally distant (Fuchs & Gehring, 2017, Luitel, Vanpée, & De Moor, 2016). Differences in methodology aside, such ratings seek to capture a sovereign entity's ability and willingness to honor debt obligations in full and on time. Investors reference sovereign credit ratings when making investment decisions in debt instruments issued by sovereign entities around the world.

We propose that a similar structure to those observed in credit rating methodologies can be applied to the challenge of evaluating cyber risk to critical infrastructure entities. A cyber capability rating (CCR) would communicate the critical infrastructure entity's *ability and willingness to mitigate discontinuous function due to cyberattack*. We preserve the phrase *ability and willingness* because it conveys not only competence or acquired proficiency of an entity to mitigate cyberattacks but said entity's readiness and intent as well. Furthermore, we present *mitigate* as the principal form of risk treatment – amongst acceptance, avoidance, transfer, and mitigation (Shameli-Sendi, Aghababaei-Barzegar, & Cheriet, 2016) – to emphasize risk reduction actions that are within direct control of the entity. Finally, we introduce the concept of *discontinuous function* to represent discrete incidents where an entity experiences discontinuity in provision of a National Critical Function (NCF) across all operations and locations. NCFs are defined by the Cybersecurity & Infrastructure Security Agency

(CISA, 2019) as "functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." Integrating this framing, we assume a discontinuity can be achieved by any of the aforementioned disruption, corruption, or dysfunction failure modes for all 55 NCFs that are individually defined by CISA (2020b).

As with sovereign credit ratings and default events, CCRs will have an inverse relationship with the negative outcome of concern. A high CCR would indicate low likelihood of discontinuous function due to cyberattack, while a low CCR would indicate high likelihood of discontinuous function due to cyberattack. Additionally, the proposed rating process measures a dependent variable that is agnostic of severity and duration through the discontinuity characterization. This is further parallel to default events where a missed payment of principal or interest by the debtor is considered a default regardless of severity or expected time in default (Bhatia, 2002). In this manner, default is treated as a predominantly static designation that precedes consequence in the classic risk equation (1) and a credit rating solely describes the likelihood element.

$$(1) \quad Risk = \mathrm{P}(occurrence) \times E[consequence|occurrence]$$

Given our domain is cybersecurity, we should also note that the likelihood element of equation (1) is often decomposed into threat and vulnerability components represented by equation (2) when articulating cyber risk.

$$(2) \quad Risk = P(threat) \times P(vulnerability|threat) \times E[consequence|threat,vulnerability]$$

There exists some acknowledgement of *threat* in credit rating methodologies, such as HR Ratings' (2017) scenario stress conditions, that lends feasibility to the aforementioned decomposition. Yet, the observed operations are neither linear or conditional and remain at the abstraction of likelihood in their implementation. Remaining at this level of abstraction is further supported by the Basel Committee on Banking Supervision's (2023) interpretation of risk which maps ratings from external credit assessment institutions (ECAIs), i.e. rating agencies, to a percentage value that is equivalent to probability of default.

Given these observations, CCRs remain at the level of abstraction of equation (1); and observing long-run rating transitions permits derivation of a *probability of discontinuity* (PD) estimate per distinct CCR designation. Figure 1 illustrates the relation between CCR and PD rating artifacts and elements of the classic risk equation (1).

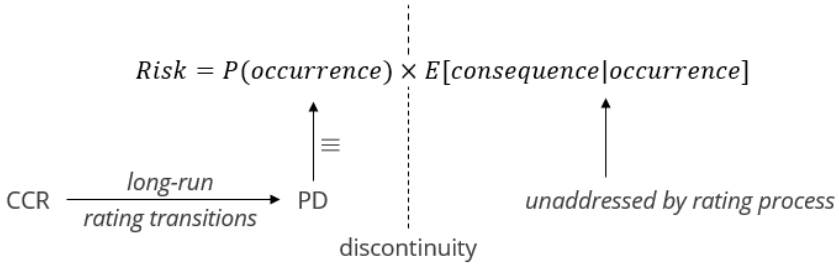

Fig. 1. Relation Between Rating Artifacts and Risk Elements

Within this context, we propose a CCR with detailed components can be consulted by critical infrastructure stakeholders to make informed cybersecurity investment decisions. To generate such a rating, we contribute a novel criterion and three-phase methodology for measuring and

communicating the likelihood element of cyber risk. The methodology is sequentially composed of baseline quantitative indicators organized by distinct capability frames, a bounded qualitative adjustment per frame, and a greater-bounded qualitative adjustment spanning the entire process. To document our contributions, the paper is organized as follows: Section 2 outlines the structure of sovereign credit ratings, Section 3 describes the criterion for detection, Section 4 defines the complete methodology, Section 5 discusses extensions in the context of risk and other domains, Section 6 details limitations and future work, and Section 7 provides concluding remarks.

2. STRUCTURE OF SOVEREIGN CREDIT RATINGS

Six NRSRO sovereign methodologies (DBRS Morningstar, 2022, Fitch Ratings, 2022, S&P Global Ratings [S&P], 2022, Japan Credit Rating Agency [JCR], 2021, Kroll Bond Rating Agency [KBRA], 2021, HR Ratings, 2017), one NRSRO general methodology (AM Best, 2020), and one CRA sovereign methodology (Scope Ratings, 2022), all open source[1], were reviewed to identify common organizational trends and procedural flows used by rating agencies. We observe that most methodologies exhibit four sequential stages: thematic organization, quantitative baseline, theme-specific adjustment and aggregation, and global adjustment. The four stages are illustrated in Fig. 2 with a notional body of elements representing the internal structure.

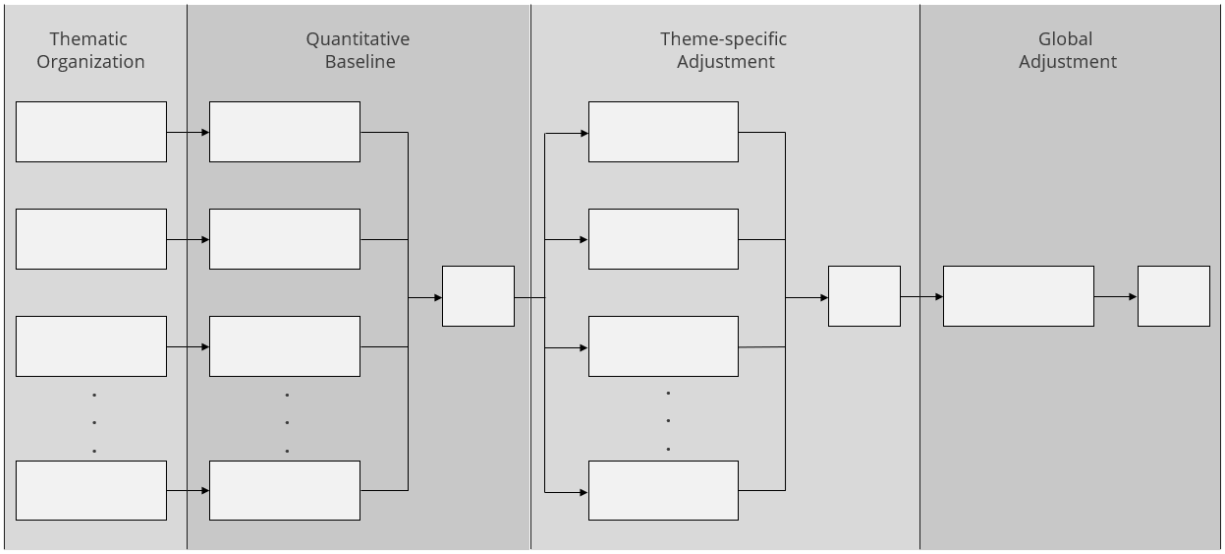

Fig. 2. Sequential Stages of Credit Rating Methodologies

2.1. Thematic Organization

Thematic organization of the assessment process into discrete sub-assessments is the first stage. The number of themes within surveyed methodologies range from 4 to 7, with a mode of 4, and median of 4.5. Themes are composed to be mutually exclusive, collectively exhaustive, and capture broad causality. Examples of themes selected from several methodologies include "fiscal base," "economic policies," "balance of payments," "structural features," and "public finances."

2.2. Quantitative Baseline

In the second stage, a quantitative baseline is typically established per theme, then aggregated across themes, based upon modeling of quantitative indicators. The number of quantitative indicators within NRSRO and CRA sovereign methodologies range from 17 to 29, with a mode of 18, and a median of 20.5. One exception to this observation is S&P (2022) which uses a mix of qualitative and quantitative factors to generate a baseline. Examples of indicators selected from several methodologies include "GDP per capita," "rate of inflation," "credit growth," "unemployment %," and "share in world GDP."

[1] KBRA was open-source at the time of initial access.

Mathematically, generating a quantitative baseline either takes the form of a singular model encompassing all indicators or 4 – 6 parallel models that are subsequently aggregated. Fitch Ratings (2022) exemplifies implementation of a singular model through use of ordinary least squares (OLS) regression to generate a baseline agnostic of organizing themes; while DBRS Morningstar (2022), Scope Ratings (2022), S&P (2022), KBRA (2021), and HR Ratings (2017) exemplify use of parallel, theme-specific models to generate a baseline. Of note, JCR (2021) does not provide any detail regarding mathematical operations.

Within the parallel modeling approach, further distinctions arise. DBRS Morningstar (2022), Scope Ratings (2022), and HR Ratings (2017) standardize intra-model indicators to respective measurement scales then perform weighted linear combination (WLC[2]) of said indicators to generate per-model outputs. These model outputs are subsequently aggregated through another WLC operation to generate a baseline; DBRS Morningstar (2022) aside, which uses simple addition post-qualitative adjustment. Conversely, S&P (2022) and KBRA (2021) standardize model outputs, not indicators, to respective measurement scales then perform WLC operations to generate a baseline. The exact value of weights used in WLC operations is often clearly articulated by sovereign methodologies, with exceptions from Scope (2022) and KBRA (2021) at the indicator level, and HR Ratings (2017) at both the indicator and model levels of abstraction.

With either singular or parallel modeling approaches, conducting analysis with respect to peer groups is another common phenomenon. Implicitly, peer comparison occurs at the transformation of time-series data to indicators (e.g. latest percentile rank) or through the implementation of standardization operations. Scope Ratings (2022) exemplifies this latter form of peer comparison through use of a minimum-maximum algorithm to rank the performance of a sovereign's indicators, individually, against a population of 125 sampled sovereigns after excluding outliers through mean absolute deviation (MAD). Explicitly, peer group considerations are mentioned by several methodologies. DBRS Morningstar (2022), Fitch Ratings (2022), Scope Ratings (2022), and KBRA (2021) either contextualize the term or define peer groups for assessment guidance. DBRS Morningstar (2022) and Scope Ratings (2022) both specify that intra-process indicative rating ranges permit accounting of the *relative strengths and weaknesses* of a sovereign in relation to peers; where Scope Ratings (2022) defines the indicative range to include the initial rating level and two adjacent levels (positive and negative). Perhaps most explicitly, KBRA (2021) defines advanced industrial (AI) and emerging market (EM) peer groups which alters the indicators and WLC weights used by the methodology.

2.3. Theme-specific Adjustment

With a baseline established, the third stage is to conduct theme-specific adjustments that are qualitative in nature, bounded in magnitude, and conducted in parallel (with exception of AM Best (2020) being linear). The number of opportunities for adjustment within surveyed methodologies range from 1 to 15, with a mode of 4, and median of 4. The bounds per adjustment opportunity are most often symmetric with integer-based steps between [-1,+1], [-2,+2], or [-3,+3] possible; where [-2,+2] is most common. However, some bounds are asymmetric and permit greater negative adjustments such as -3 or -4 attainable with only +1 on the positive side. This is observed in S&P (2022) and AM Best (2020) methodologies. No methodologies permit asymmetric positive adjustment. Furthermore, while the integer-based adjustment steps are most often commensurate with movement on respective measurement scales (e.g. +1 being a 1-unit increase), DBRS

[2] We use the term WLC to include simple average operations with uniform weights.

Morningstar (2022) and Scope Ratings (2022) use intra-theme adjustments associated with unit movements derived from proprietary measurement scales.

Aggregation of theme-specific adjustments is often a concise additive or average mathematical operation for all surveyed methodologies. Fitch Ratings (2022) and Scope Ratings (2022) display unique aggregation mechanisms by bounding the addition of theme-specific adjustments within a maximum range of [-3,+3]. Additionally, as introduced in Section 2.2, theme-specific adjustments are often conducted based upon explicit peer group comparison that is exemplified by DBRS Morningstar (2022), Fitch Ratings (2022), Scope Ratings (2022), and KBRA (2021) methodologies.

2.4. Global Adjustment

The final sequential stage is to conduct a global adjustment that is qualitative and bounded. This is solely observed in S&P (2022) and DBRS Morningstar (2022) methodologies, where a distinct qualitative adjustment exists at the culmination of the assessment process[3] that is separate from prior theme-specific adjustments. There is only one adjustment opportunity at this stage and the observed bounds are symmetric at [-1,+1] and [-2,+2], respectively.

2.5. Rating Scale

The output of every surveyed methodology is a singular value of assessment that ranges from levels "AAA" to "C" on an ordinal rating scale, where "AAA" communicates the highest ability and willingness to honor debt obligations in full and on time. A 21-level, non-default scale in Table 1 is most commonly used by rating agencies (Fitch Ratings, 2022, KBRA, 2022, S&P, 2021, AM Best, 2020), though, 19-level, non-default scales are also employed (Scope Ratings, 2022, HR Ratings, 2017, JCR, 2014) with the primary difference being the removal of plus and minus modifiers within the "CCC" region of the scale. The rating "D" is not predictive and is reserved for sovereigns in a state of active default.

Table I: Common Non-Default Scale

Level	Rating
21	AAA
20	AA+
19	AA
18	AA-
17	A+
16	A
15	A-
14	BBB+
13	BBB
12	BBB-
11	BB+
10	BB
9	BB-
8	B+
7	B
6	B-
5	CCC+
4	CCC

[3] For the purpose of this paper, we did not consider any adjustment between foreign currency and local currency debt as a distinct stage.

3	CCC-
2	CC
1	C

Furthermore, a broad distinction arises when connecting rating levels to the measurement process outlined in Sections 2.2 through 2.4. Fitch Ratings (2022), AM Best (2020), and HR Ratings (2017) use ordinal rating levels that directly match the integer levels of measurement from quantitative baseline and theme-specific adjustment stages. Other agencies such as KBRA (2022), DBRS Morningstar (2022), Scope Ratings (2022), and S&P (2021) use the same ordinal rating levels but define measurement regions through proprietary standardization; e.g. a proprietary region of 84-87 corresponding with rating level 16 in Table I. Finally, and uniquely, Fitch Ratings (2022) and S&P (2021) each preserve a subset of lower levels on respective rating scales that are exclusively qualitatively assigned.

Ratings published according to Table I are validated annually by the disclosure of single-year, multi-year, and cumulative transition matrices which display the frequency that ratings change between levels or result in default. These disclosures are mandatory for all ECAI's under the Basel Committee on Banking Supervision's (2023) regulatory framework. The cumulative frequency that ratings result in default is often meaningfully differentiated between distinct rating levels; as Bhatia (2002) illustrates a near-constant increase to default probability as ratings descend from AAA to CCC.

3. DISCONTINUITY INCIDENT CRITERION

To measure the concept of discontinuous function introduced in Section 1, we reviewed CSIS, Carnegie Endowment for International Peace (CEIP), GAO, Congressional Research Service (CRS), and Cyentia Institute repositories to identify discontinuity incidents. From a quantitative perspective, we posit such incidents occur at the extremum of a given resilience curve where NCF provision reaches zero due to cyberattack – illustrated by the solid black line in Fig. 3.

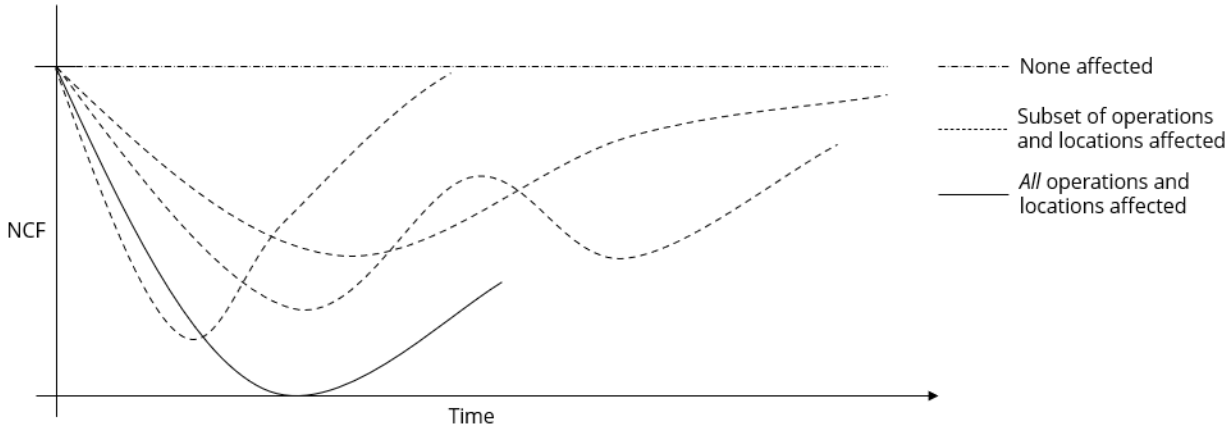

Fig. 3. Notional Resilience Curves due to Cyberattack

The initial objective was to identify incidents where language from primary or secondary sources indicated any magnitude of NCF discontinuity by an entity (assuming multiple NCFs can be provided). The CSIS (2022) timeline of significant cyber incidents and CEIP (2023) timeline of cyber incidents involving financial institutions were both reviewed through December 2022; the term "critical infrastructure cyber" was searched within GAO, CRS, and Cyentia Institute (2023) search engines; and 28 terms were searched within the Google search engine. Reviewed documents spanned the first 50 GAO "report" and "testimony" results, 47 CRS "report" results, the top 100 Cyentia Institute results, and the top 60 results per Google search term. Overall, literature review across these five sources identified a total of 58 candidate incidents across North America and Europe.

From this population, 12 incidents were removed due to operations that had no clear relation to NCFs, simple cut Internet connection mitigations, solely email system offline consequences, or insufficient open-source data to determine. This resulted in a list of 46 incidents that exhibited discontinuous function across either a subset or all entity operations and locations. Subsequently, the 18 incidents where a subset[4] was affected were removed, which resulted in the final list of 28 *discontinuity incidents* that are captured in Table II. The following Fig. 4 outlines this sequential search strategy.

[4] Subset encompasses the intermediate continuum of affected entity operations and locations from all to none without further refinement.

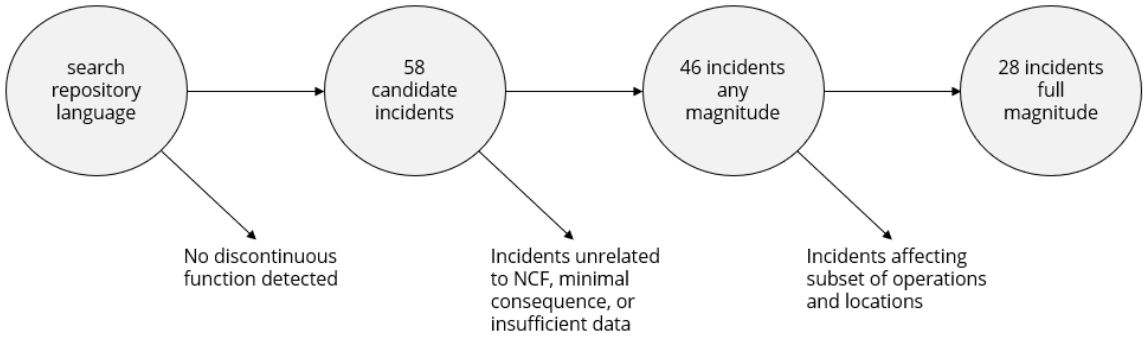

Fig. 4. Strategy for Identifying Discontinuity Incidents

Discontinuity incidents in Table II span 19 of 55 NCFs and include at least disruption (e.g. CSX) and dysfunction (e.g. steel mill) failure modes introduced by CISA (2019). Language regarding system shutdowns/outages, inaccessible services, or asset damage/replacement supported manual detection. Furthermore, akin to default, discontinuities are agnostic of severity and duration as introduced in Section 1. With respect to severity, neither geographic service region nor perceived entity importance alter the discontinuity designation. For example, no distinction is made between the cyberattack that impacted global operations of A.P. Møller-Maersk and the cyberattack that impacted regional operations of Colonial Pipeline, rather, both were comprehensive in nature. With respect to duration, the discontinuity designation spans incidents that range from minutes to months, from Estonian banks halting service 45-90 minutes to the U.S. Department of Commerce Bureau of Industry and Security re-constituting its computing network over months.

Table II: Discontinuity Incidents

Date	Sovereign	Entity	Consequence	NCF
Mar 1997	United States	Worcester Air Traffic Control	Telephone service, main radio transmitter, and runway lights shut down (GAO, 2007)	Transport Cargo and Passengers by Air
Nov 2002	United States	Earle Naval Weapons Station	Network of 300 computers shut down 1 week (GAO, 2004, U.S. Department of Justice 2002)	Provide Material and Operational Support to Defense
Nov 2002	United States	Military District of Washington	Network rendered inoperable (GAO, 2004, U.S. Department of Justice 2002)	Provide Material and Operational Support to Defense
Jan 2003	United States	Davis-Besse Nuclear Plant	Safety monitoring system disabled 5 hours; process computer failed 6 hours (GAO 2007, GAO 2006)	Generate Electricity
Jan 2003	United States	Emergency Call Center	Disrupted for several hours; served 2 police stations and at least 14 fire stations (GAO 2005)	Prepare for and Manage Emergencies; Provide Public Safety
Aug 2003	United States	CSX Transportation	Signaling, dispatching, and other systems shut down; train service cancelled or delayed up to 6 hours (GAO 2007, Information Week, 2003)	Transport Cargo and Passengers by Rail
Aug 2003	United States	Maryland Vehicle Administration	Shut down computer systems (GAO, 2004)	Operate Government
Apr 2007	United States	Department of Commerce BIS	Network offline for several months (CSIS, 2022); hardware and software replaced (Brenner, 2007)	Operate Government
May 2007	Estonia	Hansabank	online banking halted 45-90 mins; foreign money transfers unavailable (Pamment et al., 2019)	Provide Consumer and Commercial Banking Services

May 2007	Estonia	SEB Eesti Uhisbank	online banking halted 45-90 mins; foreign money transfers unavailable (Pamment et al., 2019)	Provide Consumer and Commercial Banking Services
Jan 2011	Belgium	European Commission ETS	Trading temporarily shut down (CSIS 2022, Roberts, 2011)	Provide Capital Markets and Investment Activities
Dec 2014	Germany	Steel Mill	Control system disrupted; massive physical damage (Becker, 2015, Hemsley & Fisher, 2018)	Provide Metals and Materials
Jul 2015	United States	Joint Chiefs of Staff	Network shut down; hardware and software replaced over 2 weeks (Martin, 2016)	Provide Material and Operational Support to Defense
Dec 2015	Ukraine	Chernivtsi Oblenergo	Power outage up to 6 hours, remote access to substations disrupted (Whitehead, 2017)	Distribute Electricity
Dec 2015	Ukraine	Prykarpattia Oblenergo	Power outage up to 6 hours, remote access to substations disrupted (Whitehead, 2017, Assante, 2016)	Distribute Electricity
Dec 2015	Ukraine	Kyiv Oblenergo	Power outage up to 6 hours, remote access to substations disrupted (Whitehead, 2017, Assante, 2016)	Distribute Electricity
Jun 2017	Denmark	A.P. Møller-Maersk	Network shut down; all 1,200 critical business applications inaccessible including booking and port loading systems; 76 port terminals inoperable for days; 4,000 servers and 45,000 PCs replaced over 10 days (Capano, 2021, Swinhoe, 2019, Greenberg, 2018)	Transport Cargo and Passengers by Vessel; Maintain Supply Chains
Dec 2019	United Kingdom	Travelex	All systems shut down, online exchange service inaccessible up to 1 week (Goodwin, 2020, Hussain & Ridley, 2020)	Provide Payment, Clearing, and Settlement Services
Sep 2020	Germany	Dusseldorf University Hospital	Systems disrupted for 1 week, unable to access data, patients re-routed, operations halted (AP, 2020)	Maintain Access to Medical Records; Provide Medical Care
Oct 2020	United States	UVM Health	Patient portal inaccessible (Jercich, 2020)	Maintain Access to Medical Records
May 2021	United States	Colonial Pipeline	Pipeline shut down for 5 days (Kerner, 2022)	Transport Materials by Pipeline
May 2021	Belgium	Belnet	Network offline for hours; online service inaccessible for 200 institutions (Montalbano, 2021)	Provide Internet Based Content, Information, and Communication Services
May 2021	Norway	Volue	All critical business applications shut down up to 5 days; software service to 200 water municipalities disrupted (Stupp, 2021)	Provide Information Technology Products and Services
May 2021	Ireland	HSE National Health Service	Information systems shut down and took up to 4 months to restore all servers and applications; many hospital appointments cancelled (PwC, 2021)	Maintain Access to Medical Records
Jan 2022	United States	County Government	Computer systems shut down; public office locations closed (FBI, 2022)	Operate Government
Sep 2022	Albania	Government	Total Information Management System (TIMS) shut down for 24 hours at seaports, airports, and border posts (Elezi & Gholami, 2022, Al Jazeera, 2022)	Maintain Supply Chains
Nov 2022	Denmark	Supeo	Servers shut down; enterprise asset management software inoperable (Kovacs, 2022)	Provide Information Technology Products and Services
Nov 2022	Denmark	DSB State Railway	All trains halted for several hours (Kovacs, 2022)	Transport Cargo and Passengers by Rail

The incidents in Table II represent low-frequency high-consequence cyberattacks, with over half taking place since 2015 – a possible trend. Additionally, note that discontinuities in Table II can either be achieved by the threat actor or incurred proactively by the target entity. Pre-emptive response actions by an entity to shut down operations during cyberattack are also characterized as discontinuous function.

4. METHOD FOR RATING GENERATION

To generate CCRs, we propose a rating process that is adapted from the sovereign credit structures outlined in Section 2 where, similarly, validity can be measured through detection of discontinuity incidents described in Section 3. The rating process is illustrated by Fig. 5 where BCCR, ICCR, and FCCR stand for Baseline-, Intermediate-, and Final-CCR outputs, respectively; and the titles of Core Indicators, Idiosyncratic Adjustment, and Global Adjustment correspond to three phases of baseline quantitative indicators organized by capability frames, bounded qualitative adjustment per frame, and greater-bounded qualitative adjustment per process as introduced in Section 1.

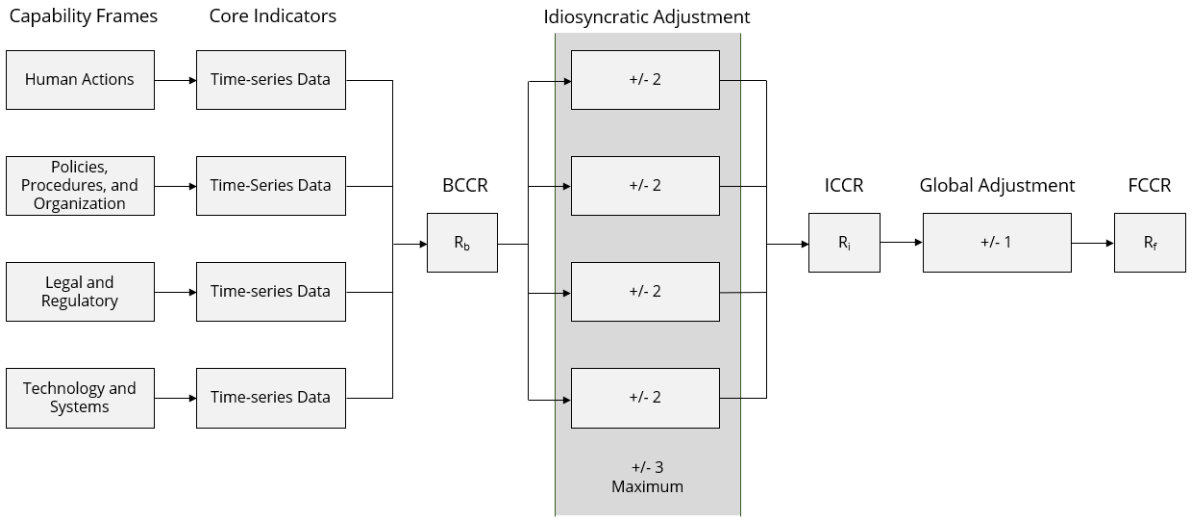

Fig. 5. Complete Structure of Rating Process

We preserve the idiosyncratic adjustment bounds of [-2,+2] as this is the most frequently observed symmetric range within surveyed methodologies. Moreover, we maintain the idiosyncratic maximum bound of [-3,+3] to emphasize the importance of an accurate quantitative baseline and to limit traversal of the CCR scale in Section 4.4. Finally, we preserve the global adjustment bounds of [-1,+1] based upon the assertion that greater distance within the process from the quantitative baseline should permit a decreasing magnitude of qualitative adjustment. The following Sections 4.1 – 4.4 detail the rationale and individual elements of the rating process and are presented in similar order to Sections 2.1 – 2.5 for ease of reference.

4.1. Capability Frames

Capability frames (i.e., themes) are defined to be mutually exclusive, collectively exhaustive, and capture broad causality. Through open-ended literature review, four sources[5] that holistically categorize cybersecurity concepts were selected for inductive content analysis. Global Cyber Security Capacity Centre (GCSCC, 2021); United Nations International Telecommunication Union (UN ITU, 2015); Romanosky, Ablon, Kuehn, and Jones (2019); and Cebula and Young (2010) were analyzed to identify organizing concepts used by each source and associated membership of

[5] Overall, it was rare to find any source that conducted abstract and holistic categorization.

concepts to induced capability frames. Table III displays the alignment of organizing concepts to capability frames.

Furthermore, the language content of each source was synthesized to derive definitions for each of the four capability frames. The definitions are:

- **Human Actions:** the extent to which staff participate in knowledge development, respond competently to cyber incidents, and promote a culture of cybersecurity.
- **Policies, Procedures, and Organization:** the maturity of internal processes and structures for implementing and managing cybersecurity.
- **Legal and Regulatory:** adherence to applicable laws, regulations, and standards; and extent of participation in formal and informal cooperation networks regarding cybersecurity.
- **Technology and Systems:** the extent of deployed hardware, software, and effectiveness of their resultant integration to enhance entity-wide cybersecurity.

Table III: Alignment of Concepts to Capability Frames

Publication	Organizing Concept	Human Actions	Policies, Procedures, and Organization	Legal and Regulatory	Technology and Systems
GCSCC (2021)	Policy and Strategy		X		
	Culture and Society	X			
	Knowledge and Capability		X		
	Legal and Regulatory Frameworks			X	
	Standards, Organizations, and Technologies		X		X
UN ITU (2015)	Legal Measures			X	
	Technical Measures				X
	Organizational Measures		X		
	Capacity Building	X	X		
	Cooperation			X	
Romanosky, Ablon, Kuehn, and Jones (2019)	Organization		X		
	Technical				X
	Policies and Procedures		X		
	Legal and Compliance			X	
Cebula and	Actions of People	X			

Young (2010)	Systems & Technical				X
	Internal Processes		X		
	External Events		X	X	

4.2. Core Indicators

Core indicators are defined to be quantitatively measured time-series that share causal relation to respective capability frames. Through extending the prior open-ended literature review, ten sources were selected for deductive content analysis to identify a representative set of discrete artifacts used in some capacity to assess cybersecurity. Six foundational sources included those within commercial rating (BitSight, 2022, Sohval, 2020, RiskRecon 2020), insurance (Romanosky et al., 2019), and supranational governance (GCSCC, 2021, UN ITU, 2015) paradigms. Four supplemental sources included Ruan (2017) and Convercent (2016) which provide lists of assessment artifacts, Cebula and Young's (2010) exhaustive taxonomy, and CISA's (2020a) comprehensive review of per-incident costs. Artifacts identified within the commercial rating paradigm were weighed with particular importance as their aggregation of time-series data to produce a single index value most resemble the mathematical operations that sovereign credit rating processes use in Section 2.2. Analysis of these ten sources led to identification of 184 non-unique assessment artifacts.

In addition to identifying artifacts, several guiding principles arose from literature review that were used to inform indicator selection and definition. These principles are:

- **Existence and number:** used by the UN ITU (2015), indicators may be derived from the existence or normalized number of phenomena.
- **Median centrality:** median is the preferred measure of central tendency due to the significant skewing effect that outliers can have on the mean. This is supported by CISA's (2020a) decision to weigh median more than mean in their analysis of per-incident cyber costs.
- **Entity control:** indicators should capture actions that are within direct control of the entity being evaluated. This enables an entity to exert improvement in their *ability and willingness* to mitigate discontinuous function due to cyberattack.

Subsequently, indicators were manually derived based upon artifact saturation across multiple sources and guiding principles. Derivation was validated through a series of discussion sessions with subject matter experts who had prior responsibility for cyber incident response and/or managing cybersecurity solutions at various firms. Table IV displays the final set of 29 quantitative indicators with seven, nine, five, and eight indicators distributed across distinct capability frames.

Additionally, a separate and independent literature review was conducted to identify exact or proximate publication of indicators proposed in Table IV – where *exact* refers to sources that publish data matching our explicit definitions and *proximate* refers to sources that publish data which either imply or are a subset of our definitions. The review encompassed 33 terms within the Google search engine and investigation of the top 60 results per term. We find 16 of 29 indicators are collected and published in some form, usually ranges or point-estimates. Though, all indicators are published at the population-level which is one level of aggregation higher than the requisite entity-

level time-series. The results of this review are captured in Table IV as well, with "*ex.*" or "*prox.*" noted next to each source.

Table IV: Complete Set of Core Indicators

Indicator	Type	Definition	Exact or Proximate Source
Human Actions			
Percent of cybersecurity staff certified by recognized programs	Decimal	Percent of entity cybersecurity staff certified by recognized programs. Recognized programs may include university degrees, vendor-specific certification, and industry-, sovereign-, or supranational-based accreditation schemes.	ISC2 (2022) ex.
Percent of staff who participate in regular cybersecurity training	Decimal	Percent of entity staff who participate in cybersecurity training at a planned cadence through any number of channels such as virtual lessons, in-person instruction, or conferences.	EY (2022) prox.
Percent of staff who receive regular cybersecurity communications	Decimal	Percent of entity staff who receive cybersecurity communications at a planned cadence. Communications may be proactive or pushed and include industry reports, threat intelligence, vulnerability notifications, or security alerts.	-
Median time-to-detect	Decimal	Median time from cyberattack occurrence to detection by entity staff.	Baker Hostetler (2022) ex. Audit Analytics (2022) ex. Verizon (2022)[6] ex.
Median time-to-contain	Decimal	Median time from cyberattack detection to containment of the threat actor.	Baker Hostetler (2022) ex. Cisco (2021) prox.
Median time-to-notification	Decimal	Median time from cyberattack detection to notification of affected customers and/or regulators.	Baker Hostetler (2022) ex. Audit Analytics (2022) ex.
Median time-to-completion	Decimal	Median time from cyberattack containment to completion of incident-related actions. This may include forensics, knowledge management, staff briefings, and technology configuration updates.	-
Policies, Procedures, and Organization			
Existence of entity-wide response organization	Binary Integer	Existence of an entity-wide response organization such as Security Operations Center (SOC), Computer Emergency Response Team (CERT), Cyber Incident Response Team (CIRT), or Cyber Security Incident Response Team (CSIRT).	Marsh McLennan (2023) ex.
Existence of executive-level information security officer or executive-level team for strategy development and implementation	Binary Integer	Existence of executive-level information security officer or executive-level team for strategy development and implementation, e.g. permanent committee, working group, or advisory council.	EY (2022) ex.
Existence of entity-wide disclosure mechanisms	Binary Integer	Existence of entity-wide disclosure mechanisms such as vulnerability reporting, insider threat, or whistleblower channel.	-

[6] It is worth noting that the VERIS Community Database does collect incident-level time-to-detect and time-to-contain indicators, from which Verizon's aggregate statistics are derived.

Percent of entity-wide policies and procedures developed and implemented	Decimal	Percent of entity-wide policies developed and implemented from the following list: __ Internal standardization (e.g. best-practice, guidelines, standards) __ Business continuity or disaster recovery plans __ Breach or incident response plans __ Data collection, retention, and destruction __ Service level agreements __ Password requirements and guidance __ Staff procurement of third-party software applications __ Software application usage (third-party and proprietary)	EY (2022) prox. Cisco (2021) prox.
Median review cadence of entity-specific training materials	Decimal	Median review cadence of training materials developed and disseminated by the entity or on behalf of the entity by a third-party.	-
Median review or exercise cadence of policies and procedures	Decimal	Median review or exercise cadence of proprietary policies and procedures developed and disseminated by the entity. Exercises may be appropriate for simulated response of event-driven policies and procedures.	EY (2022) prox.
Percent of policies and procedures with current, individual staff responsible for ownership	Decimal	Percent of policies and procedures with a current, individual staff member responsible for ownership. Responsibilities may include periodic review, version control, and issue escalation.	-
Percent of technology budget allocated to cybersecurity	Decimal	Percent of (information and operational) technology budget allocated to cybersecurity.	Hiscox (2022) ex.
Percent of cybersecurity budget allocated to proactive measures	Decimal	Percent of cybersecurity budget allocated to proactive measures such as threat intelligence, threat hunting, red-teaming, and vulnerability discovery.	-
Legal and Regulatory			
Median review cadence for adherence to third-party and supplier standards	Decimal	Median review cadence for adherence to third-party and supplier standards which the entity depends upon.	-
Median review cadence for adherence to requirements of jurisdiction enforcement, prosecution, and court bodies	Decimal	Median review cadence for adherence to requirements of jurisdiction enforcement, prosecution, and court bodies applicable to the entity.	-
Median review cadence for integration of recognized cybersecurity frameworks	Decimal	Median review cadence for integration of recognized cybersecurity frameworks into entity operations. Recognized frameworks may originate from industry, academic, sovereign, or supranational entities.	EY (2022) prox.
Number of cross-entity or sector-specific benchmarking exercises participated in	Decimal	Number of cross-entity or sector-specific benchmarking exercises participated in to measure peer group performance.	-
Number of partnerships, cooperative frameworks, and asset-sharing agreements for cybersecurity	Decimal	Number of partnerships, cooperative frameworks, and asset-sharing agreements currently participating in for cybersecurity. Participation may be unilateral or multilateral. Assets may include information, technology, expertise, or resources.	EY (2022) prox.
Technology and Systems			
Median time from disclosure-to-patching of CVEs in proprietary software	Decimal	Median time from disclosure to patching of publicly reported Common Vulnerabilities and Exposures (CVEs) in proprietary entity software.	Verizon (2022) prox.

Median time from release-to-update of third-party software and operating systems	Decimal	Median time from release to update of third-party software and operating systems which the entity depends upon.	-
Percent of email traffic secured by SPF and DKIM measures	Decimal	Percent of entity email traffic secured by Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM) measures.	-
Percent of network ports that are unfiltered with accessible services	Decimal	Percent of entity network ports that are unfiltered with services accessible to potential threat actors.	-
Percent of Internet communications encrypted by TLS	Decimal	Percent of Internet communications encrypted by the latest Transport Layer Security (TLS) protocol.	-
Percent of software applications that use identities administered by a centralized service	Decimal	Percent of software applications that grant access and privileges based upon identities administered by a centralized identity and access management (IAM) service.	Accenture (2019) prox.
Percent of automated security measures implemented	Decimal	Percent of entity-wide automated security measures implemented from the following list: __ Endpoint encryption __ Multi-factor authentication __ Web application firewall __ Network firewall(s) __ Log aggregation, analysis, and alerting __ Anti-malware system __ Anti-intrusion system __ Data backup	Accenture (2019) prox. Marsh McLennan (2023) prox.
Existence of secure VPN for staff remote access and site-to-site connection	Binary Integer	Existence of secure Virtual Private Network (VPN) for remote access by entity staff and site-to-site connection between entity networks.	Kochovski (2023) ex.

4.3. Idiosyncratic and Global Adjustments

Qualitative adjustments offer the opportunity to account for epistemic uncertainty not sufficiently modeled by core indicators. This is conducted per capability frame at the Idiosyncratic Adjustment phase and per rating process at the Global Adjustment phase illustrated in Fig. 5. In defining qualitative adjustment tiers, the objective was to replicate the structure and amount of language (often several sentences to paragraphs) in NRSRO and CRA sovereign methodologies while using appropriate cybersecurity terminology. Moreover, a structure and amount of language that is similar to NIST's (2018) description of implementation tiers in the Cybersecurity Framework.

Each integer-based tier is several sentences composed of subjects and heuristics. *Subjects*, per capability frame, were synthesized from frame definitions, indicator definitions, and Cebula and Young's (2010) taxonomy. Examples of subjects include "incident response," "process design," and "review mechanisms." *Heuristics* were derived from content analysis of the GCSCC's (2021) maturity model where we identified 511 non-unique clauses that describe a capability state. Heuristic clauses primarily consist of verb phrases and adjective phrases, but noun phrases are also present and in such cases the clause was reduced or simplified to remain broadly applicable. Examples of heuristics include "habitual," "anticipatory," and "minimal to none." Fig. 6 illustrates the sentence structure of qualitative adjustment tiers through combination of subjects and heuristics with an example extracted from Table V.

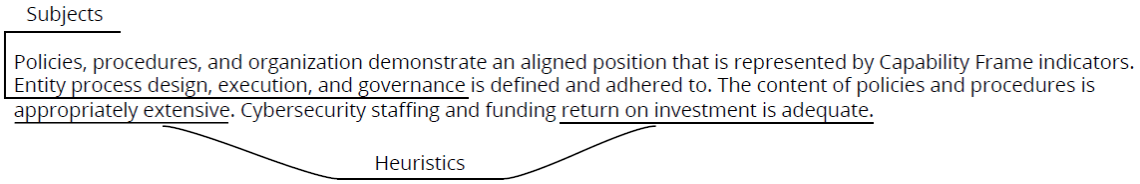

Fig. 6. Structure of Qualitative Adjustment Tiers

With a set of subjects and heuristics, qualitative language was manually generated for each of the 20 idiosyncratic adjustment tiers and 3 global adjustment tiers. The first sentence of each tier further emphasizes the objective of each phase – idiosyncratic adjustment is solely respective to the given capability frame and global adjustment is respective to the entire rating process. Table V catalogs the final set of 23 qualitative adjustment tier definitions.

Table V: Complete Set of Idiosyncratic and Global Adjustment Tiers

Value	Tier	Definition
Idiosyncratic Adjustment		
Human Actions		
+2	Highly Advantaged	Human actions demonstrate a highly advantaged position that is not fully represented by Capability Frame indicators. Entity staff engage in significant or habitual knowledge development and have a leading awareness of cyber concepts. Cyber incident response is dynamic and extensively coordinated. Management actions are rigorously understood and make rare, adaptive deviations from established strategy.
+1	Advantaged	Human actions demonstrate an advantaged position that is not fully represented by Capability Frame indicators. Entity staff engage in substantial or proactive knowledge development and have a widely informed awareness of cyber concepts. Cyber incident response may be collaborative and coordinated. Management actions are clearly understood and deviate rarely from established strategy.
0	Neutral	Human actions demonstrate an aligned position that is represented by Capability Frame indicators. Entity staff engage in adequate knowledge development and have a recognized awareness of cyber concepts. Cyber incident response is consistent. Management actions are comprehensible and deviate minimally from established strategy.
-1	Disadvantaged	Human actions demonstrate a disadvantaged position that is not fully represented by Capability Frame indicators. Entity staff engage in limited or ad-hoc knowledge development and have a cursory awareness of cyber concepts. Cyber incident response may lack consistency or coordination. Management actions lack clarity and deviate discernably from established strategy.
-2	Highly Disadvantaged	Human actions demonstrate a highly disadvantaged position that is not fully represented by Capability Frame indicators. Entity staff engage in minimal to no knowledge development and have sparse to no awareness of cyber concepts. Cyber incident response may be completely reactive or uncoordinated. Management actions are unclear and deviate frequently from established strategy.
Policies, Procedures, and Organization		
+2	Highly Advantaged	Policies, procedures, and organization demonstrate a highly advantaged position that is not fully represented by Capability Frame indicators. Entity process design, execution, and governance is adaptive, formal, and rigorously adhered to. The content of policies and procedures is deeply integrated and continuously updated. Cybersecurity staffing and funding return on investment is markedly significant.
+1	Advantaged	Policies, procedures, and organization demonstrate an advantaged position that is not fully represented by Capability Frame indicators. Entity process design, execution, and governance is formalized and consistently adhered to. The content of policies and procedures may be comprehensive and proactively updated. Cybersecurity staffing and funding return on investment is substantial.

0	Neutral	Policies, procedures, and organization demonstrate an aligned position that is represented by Capability Frame indicators. Entity process design, execution, and governance is defined and adhered to. The content of policies and procedures is appropriately extensive. Cybersecurity staffing and funding return on investment is adequate.
-1	Disadvantaged	Policies, procedures, and organization demonstrate a disadvantaged position that is not fully represented by Capability Frame indicators. Entity process design, execution, and governance is informal and inconsistently adhered to. The content of policies and procedures may lack scope or exist on an ad-hoc basis. Cybersecurity staffing and funding return on investment is insufficient.
-2	Highly Disadvantaged	Policies, procedures, and organization demonstrate a highly disadvantaged position that is not fully represented by Capability Frame indicators. Entity process design, execution, and governance is ill-defined and rarely adhered to. The content of policies and procedures has minimal to no relevance or existence. Cybersecurity staffing and funding return on investment is notably limited or administered completely reactive.
Legal and Regulatory		
+2	Highly Advantaged	Legal and regulatory demonstrate a highly advantaged position that is not fully represented by Capability Frame indicators. Entity review and communication mechanisms are exhaustive and adaptive to evolving requirements. Participation in formal and informal cooperation networks is habitual, and the entity exhibits leadership.
+1	Advantaged	Legal and regulatory demonstrate an advantaged position that is not fully represented by Capability Frame indicators. Entity review and communication mechanisms are substantial and anticipatory of requirements. Participation in formal and informal cooperation networks is frequent and proactive.
0	Neutral	Legal and regulatory demonstrate an aligned position that is represented by Capability Frame indicators. Entity review and communications mechanisms are sufficient and reflect requirements. Participation in formal and informal cooperation networks is routine and intentional.
-1	Disadvantaged	Legal and regulatory demonstrate a disadvantaged position that is not fully represented by Capability Frame indicators. Entity review and communication mechanisms are insufficient or un-aligned to requirements. Participation in formal and informal cooperation networks is limited or ad-hoc in nature.
-2	Highly Disadvantaged	Legal and regulatory demonstrate a highly disadvantaged position that is not fully represented by Capability Frame indicators. Entity review and communication mechanisms are strikingly insufficient and exhibit rare to no reflection of requirements. Participation in formal and informal cooperation networks is minimal to none in nature.
Technology and Systems		
+2	Highly Advantaged	Technology and systems demonstrate a highly advantaged position that is not fully represented by Capability Frame indicators. Entity infrastructure capacity, performance, and maintenance is considerable and dynamic. Software configuration, change control, coding, and testing practices are exhaustive and adaptive to emerging requirements. System design, specification, and integration are rigorously understood and habitually coordinated.
+1	Advantaged	Technology and systems demonstrate an advantaged position that is not fully represented by Capability Frame indicators. Entity infrastructure capacity, performance, and maintenance is substantial. Software configuration, change control, coding, and testing practices are extensive and anticipatory of requirements. System design, specification, and integration may be clearly understood and well-coordinated.
0	Neutral	Technology and systems demonstrate an aligned position that is represented by Capability Frame indicators. Entity infrastructure capacity, performance, and maintenance is adequate. Software configuration, change control, coding, and testing practices are defined and reflect requirements. System design, specification, and integration is comprehensible.
-1	Disadvantaged	Technology and systems demonstrate a disadvantaged position that is not fully represented by Capability Frame indicators. Entity infrastructure capacity, performance, and maintenance is insufficient. Software configuration, change control, coding, and testing practices are inappropriate or un-aligned to requirements. System design, specification, and integration may lack clarity or indicate limited coordination.

-2	Highly Disadvantaged	Technology and systems demonstrate a highly disadvantaged position that is not fully represented by Capability Frame indicators. Entity infrastructure capacity, performance, and maintenance is notably insufficient. Software configuration, change control, coding, and testing practices are completely inadequate or exhibit minimal to no reflection of requirements. System design, specification, and integration are decidedly unclear and uncoordinated.
Global Adjustment		
+1	Advantaged	The entity demonstrates an advantaged position that is not fully represented by the rating process. Risk management actions are substantial and anticipatory of the threat landscape, technology environment, and secular trends within the critical infrastructure sector. Volatility of indicators may be minimal.
0	Neutral	The entity demonstrates an aligned position that is represented by the rating process. Risk management actions are appropriate and consider the threat landscape, technology environment, and secular trends within the critical infrastructure sector. Volatility of indicators is within expectation.
-1	Disadvantaged	The entity demonstrates a disadvantaged position that is not fully represented by the rating process. Risk management actions are insufficient and exhibit limited recognition of the threat landscape, technology environment, and secular trends within the critical infrastructure sector. Volatility of indicators may be elevated.

4.4. Cyber Capability Rating Scale

To communicate capability, we adapt the 21-level scale from Table I to be applicable for the rating process outlined so far in Section 4. This adapted scale is represented by Table VI. Each integer-based adjustment step from Fig. 5 is commensurate with movement up or down the levels denoted in Table VI. For example, a BCCR is mathematically established at 10.25, then an idiosyncratic adjustment of -1 results in an ICCR of 9.25, and a global adjustment of -1 results in an FCCR of 8.25. Thus, the example entity would be rated as B or "highly speculative capability." Given the bounds in Fig. 5, a rating can deviate at most four levels from the quantitative baseline through qualitative adjustments.

Table VI: CCR Scale

Level	Rating	Description
21	AAA	Exemplary Capability
20	AA	High Capability
19		
18		
17	A	Upper Medium Capability
16		
15		
14	BBB	Lower Medium Capability
13		
12		
11	BB	Speculative Capability
10		
9		
8	B	Highly Speculative Capability
7		
6		
5	CCC	Substantial and Persistent Risk
4		
3		
2	CC	Serious and Embedded Risk
1	C	Extraordinary and Embedded Risk

D	Discontinuous Function

5. DISCUSSION

5.1. Completing the Risk Equation

As described in this paper, the rating process solely addresses the likelihood element of equation (1) through generation of a PD estimate by observing long-run rating transitions in Fig. 1. Yet, it is evident from Table II that severity of consequences does vary significantly beyond the static discontinuity designation. The Basel Committee on Banking Supervision's (2023) interpretation of risk, again, lends itself to addressing this gap and we decompose the consequence element of equation (1) into two components: *impact given discontinuity* (IGD) and *exposure at discontinuity* (EAD). Where, IGD is defined as the proportion of value affected by the target entity's discontinuous function; and EAD is defined as the value of the entire downstream network of entities that are dependent upon the target entity. Use of the term *dependent* in EAD is meant to convey dependency to any extent – entities that have a direct relationship with the target entity or entities that have an indirect relationship with the target entity due to their downstream supply chain position. With these two definitions introduced, we can represent the classic risk equation (1) as the product of PD, IGD, and EAD, noted by equations (3) – (5).

$$\text{(3)}\quad \mathrm{P}(occurrence) \equiv PD$$

$$\text{(4)}\quad E\left[consequence \,\middle|\, occurrence\right] \equiv IGD \times EAD$$

$$\text{(5)}\quad Risk \equiv PD \times IGD \times EAD$$

Fig. 7 further illustrates how an estimate of consequence is derived from the product of IGD and EAD.

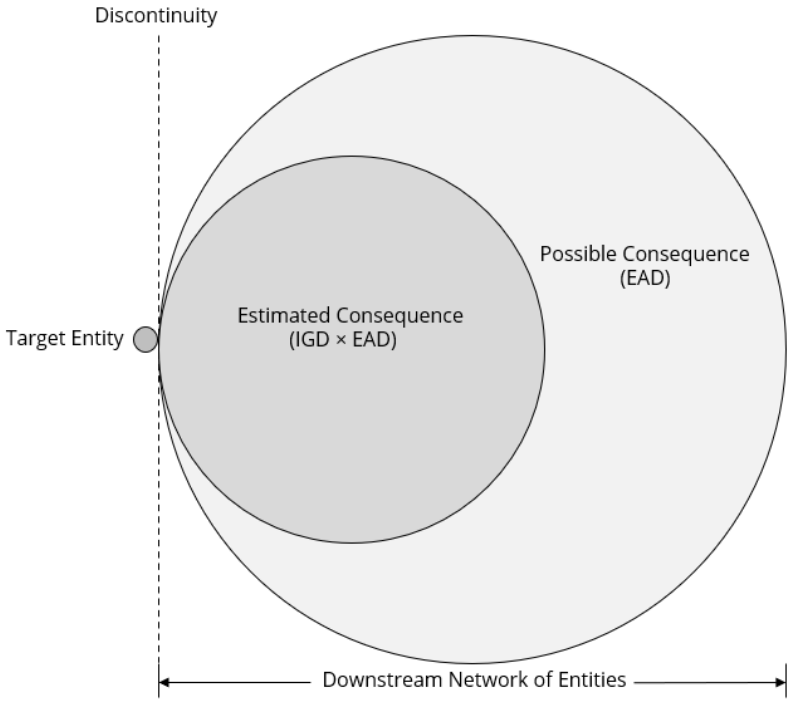

Fig. 7. Relation Between Consequence Components

Conceptually similar interpretations of consequence are provided by Welburn and Strong (2021) and Cyentia Institute (2020). Welburn and Strong (2021) define cascading cyber failures as "the result of one cyber incident propagating outward and causing many disruptions," which "lead to a domino effect across firms and organizations interconnected through supply chains." They analyze downstream impacts of the cyberattack on A.P. Møller-Maersk through novel application of input-output (I/O) modeling and find, after parameterizing for duration of 10-60 days, that potential losses may reach a maximum of $54.494 billion while estimated losses are likely to be $19.07 billion. The difference between these two monetary amounts is achieved through multiplying the maximum amount by 0.35, which is the resilience measure for A.P. Møller-Maersk's heterogeneous network of downstream entities. This mathematical operation to estimate impacts from cascading cyber failures appears reasonably analogous to the operation of quantifying EAD ($54B) and multiplying by IGD (0.35) to produce a consequence estimate.

Cyentia Institute (2020) defines multi-party cyber incidents as incidents that "not only involve the primary organization, but also generate secondary loss events that impact various other 3rd/4th/Nth parties," termed more concisely as "ripple events." They analyze the top 50 ripple events based upon reported financial losses, number of data records affected, and number of firms involved. Descriptive statistics reveal that the median number of entities impacted is 31 with a maximum of 800, and that the median financial loss is $90.4 million with a maximum of $7.3 billion. Top 50 events aside, Cyentia Institute (2020) further observes that "the median loss for multi-party incidents is over 10x that of their single-party" counterparts. The emphasis on higher-order relationships appears consistent with EAD's consideration of downstream entities, while the evidence-based magnitude of billions in monetary losses is consistent with Welburn and Strong's (2021) modeled magnitude of billions.

Across either example, the *value* referenced by IGD and EAD tends to take the form of a monetary amount. This is common and useful in decision-making, but interpretation of *value* can be flexible to include other forms of impact that result from cyberattacks such as physical, psychological, reputational, and societal (Agrafiotis, Nurse, Goldsmith, Creese, & Upton, 2018). Additionally, we assume *value* meaningfully varies per characteristics of the target entity's downstream network. This is exemplified by Shell being able to swiftly re-route oil supplies to alternate depots when Mabanaft and Oiltanking experienced discontinuity to a subset of locations (Pearson, 2022) – a nuance touched upon in I/O modeling assumptions introduced by Welburn and Strong (2021). In this case, the downstream entity Shell's adaptability would reduce IGD for Mabanaft and Oiltanking incidents. Overall, it is likely that the incident differences within Table II further fluctuate the valuation of downstream networks, i.e. which NCF and failure mode affected entity operations and locations, but we abstain from further investigating this relation to consequence.

5.2. Extension to Other Domains

The process of adapting an abstract methodology from finance to cybersecurity domains yielded several distinct insights. We posit two axioms and five investigative considerations for creating a domain-agnostic process that integrates quantitative and qualitative data to produce a singular value of assessment. The two axioms are:

- **Axiom I:** quantitative baseline precedes qualitative adjustment.
- **Axiom II:** successive phases of qualitative adjustment permit a decreasing magnitude of adjustment.

And, with Fig. 2 as reference, we posit the following investigative considerations for process structure: (1) the definition of exclusive, exhaustive, and causal themes; (2) the selection, transformation, and aggregation operations for indicators; (3) the magnitude, extent, symmetry, and definition of bounds for qualitative adjustments; (4) the extent and definition of rating scale levels; and (5) the definition and use of peer groups, and mechanisms for linking quantitative and qualitative phases within the overall process.

6. LIMITATIONS AND FUTURE WORK

Our exploratory adaptation of sovereign credit rating processes to critical infrastructure cyber risk assessment yields several clear limitations. Foremost being the reliance on manual detection of discontinuity incidents in Section 3 and manual derivation of frames, indicators, and heuristics in Sections 4.1 – 4.3. Though guided by observations from sovereign rating structures, these actions would benefit from greater algorithmic and quantifiable specification to be repeatable. A reasonable alternative for indicator derivation may be to build upon established academic surveys of security metrics (Pendleton, Garcia-Lebron, Cho, & Xu, 2016). Additionally, and related to manual outcomes, we find that the requisite time-series data to test our formulation does not publicly exist, even though expansive collaboration to generate data sets is common within the cybersecurity domain, e.g. the 87 partnerships reported by Verizon (2022). Crafting a reduced formulation that solely requires publicly available data would be a means to test validity.

With respect to the rating structure itself, other limitations arise. Alterations to the qualitative adjustment tiers such as expanded bounds, asymmetric bounds, and greater granularity should be investigated. We note this because separate analyses of internal bank rating processes find that the frequency of rating change is higher with preset weights (Brunner, Pieter, & Weber, 2000) and some banks derive 30-50% of a rating from qualitative factors (Svítil, 2018). Additionally, investigating which indicators are primary determinants of a rating would prove valuable. Sovereign credit rating literature observes that subsets of determinants often provide outsize explanation of rating variance (Afonso, Gomes, & Rother, 2011, Mellios & Paget-Blanc, 2006, Afonso, 2003, Mulder & Perrelli, 2001, Cantor & Packer, 1996) and such an investigation could aid decomposition or synthesis of indicators to appropriately distribute explanatory power. From this determinant set, exploring weighting procedures for a large amount of indicators such as analytic hierarchy process in the climate[7] domain (Krajnc & Glavic, 2005) or multi-criteria decision analysis in the cybersecurity domain (Ganin et al., 2020) would provide further value. Finally, percent- and existence-based measures may require transformation into measures of performance or utilization as capability improves amongst rated entities and such indicators become static. We do not detail any mechanisms for updating indicators and this would be necessary for the sustained use of the rating process.

[7] A cursory review of "integrated assessment" in climate literature shows wide use of methods that integrate quantitative and qualitative data to produce an estimate. Not the same as methods we propose, but of interest to this paper, nonetheless.

7. CONCLUSION

We contribute a novel, three-phase methodology for measuring and communicating the likelihood element of cyber risk that is adapted from sovereign credit rating literature. Furthermore, we demonstrate a repeatable process for translating a method across domains, finance to cybersecurity, and across levels of abstraction, sovereign- to entity-level considerations. Though, we find clear limitations in attempting to execute the methodology – mostly due to our aspirational derivation of core indicators agnostic of whether relevant time-series currently exists. Notably, the cybersecurity domain does not have a century of development to rely upon that the emergent structure of sovereign credit ratings does. Implementing our proposed rating process will require trust and partnership from a multitude of public and private entities within the cybersecurity domain. Upon achieving steady-state implementation, the unique approach of integrating quantitative and qualitative data to produce a singular value of assessment may be valuable to sovereign-scale risk management of critical infrastructure groups targeted by threat actors.

Additionally, and regardless of implementation outcomes, we contribute a novel criterion for measurement through the discontinuous function characterization. Measuring incidents as a discontinuity in provision of an NCF across all operations and locations may be adapted to other analytical processes that generate an assessment value; and we offer descriptive analysis of how both quantitative and qualitative data are sequentially modeled in the widely used analytical process of sovereign credit ratings. Furthermore, we provide 28 examples of discontinuity incidents but there are likely more that remain undetected since there are scarce incentives for victimized entities to publicly disclose shortcomings. An appropriate level of secure, public-private partnership may be a reasonable approach to facilitate detection at scale.

REFERENCES

Accenture. (2019). *The Cost of Cybercrime*. https://iapp.org/media/pdf/resource_center/accenture_cost_of_cybercrime_study_2019.pdf.

Afonso, A., Gomes, P., Rother, P. (2011). Short- and Long-run Determinants of Sovereign Debt Credit Ratings. *International Journal of Finance and Economics*, 16(1), 1-15.

Afonso, A. (2003). Understanding the determinants of sovereign debt ratings: Evidence for the two leading agencies. *Journal of Economics and Finance*, 27, 56-74.

Agrafiotis, I., Nurse, J.R.C., Goldsmith, M., Creese, S., Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, 4(1).

Al Jazeera. (2022). *Albania blames Iran for second cyberattack since July*. https://www.aljazeera.com/news/2022/9/10/albania-blames-iran-for-second-cyberattack-since-july.

AM Best. (2020). *Best's Credit Rating Methodology*. https://www3.ambest.com/ambv/ratingmethodology/.

Assante, M. (2016). *Confirmation of a Coordinated Attack on the Ukrainian Power Grid*. https://www.sans.org/blog/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid/.

Associated Press. (2020). *German hospital hacked, patient taken to another city dies*. https://apnews.com/article/technology-hacking-europe-cf8f8eee1adcec69bcc864f2c4308c94.

Audit Analytics. (2022). *Trends in Cybersecurity Breach Disclosures*. https://www.auditanalytics.com/doc/AA_Trends_in_Cybersecurity_Report_April_2022.pdf.

Baker Hostetler. (2022). *Data Security Incident Response Report*. https://www.bakerlaw.com/BakerHostetler-Launches-2022-Data-Security-Incident-Response-Report-Resilience-and-Perseverance.

Basel Committee on Banking Supervision. (2023). *The Basel Framework*. https://www.bis.org/basel_framework/index.htm.

Becker, R.A. (2015). *Cyber Attack on German Steel Mill Leads to 'Massive' Real World Damage*. https://www.pbs.org/wgbh/nova/article/cyber-attack-german-steel-mill-leads-massive-real-world-damage/.

Bhatia, A.V. (2002). *Sovereign Credit Ratings Methodology: An Evaluation*. International Monetary Fund Working Paper No. 02/170.

BitSight. (2022). *How BitSight Calculates Security Ratings*. https://www.bitsight.com/sites/default/files/2022-02/How%20BitSight%20Calculates%20Security%20Ratings.pdf.

Brenner, S.W. (2007). At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare. *Journal of Criminal Law and Criminology*, 97(2), 379-476.

Brunner, A., Pieter, J., Weber, M. (2000). *Information production in credit relationship: On the role of internal ratings in commercial banking*. Goethe University Frankfurt, Center for Financial Studies Working Paper No. 2000/10.

Cantor, R., Packer, F. (1996). Determinants and Impact of Sovereign Credit Ratings. *Economic Policy Review*, 2(2).

Capano, D.E. (2021). *Throwback Attack: How NotPetya accidentally took down global shipping giant Maersk*. https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-how-notpetya-accidentally-took-down-global-shipping-giant-maersk/.

Carnegie Endowment for International Peace. (2023). *Timeline of Cyber Incidents Involving Financial Institutions*. https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline.

Cebula, J.J., Young, L.R. (2010). *A Taxonomy of Operational Cyber Security Risks*. (CMU/SEI-2010-TN-02). Software Engineering Institute, Carnegie Mellon University.

Center for Strategic & International Studies. (2022). *Significant Cyber Incidents*. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

Cisco. (2021). *Security Outcomes Study Volume 2*. https://www.cisco.com/c/dam/en/us/products/collateral/security/security-outcomes-study-vol-2-report.pdf?ccid=cc000160&oid=rptsc027923&dtid=odicdc001478.

Convercent. (2016). *Compliance Metrics Handbook*. http://www.convercent.com/resource/convercent-guide-compliance-metrics-handbook.pdf.

Cybersecurity & Infrastructure Security Agency. (2020a). *Cost of a Cyber Incident: Systemic Review and Cross-Validation*. https://www.cisa.gov/sites/default/files/publications/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf.

Cybersecurity & Infrastructure Security Agency. (2020b). *National Critical Functions Status Update to the Critical Infrastructure Community*. https://www.cisa.gov/sites/default/files/publications/ncf-status-update-to-critical-infrastructure-community_508.pdf.

Cybersecurity & Infrastructure Security Agency. (2019). *National Critical Functions an Evolved Lens for Critical Infrastructure Security and Resilience*. https://www.cisa.gov/sites/default/files/publications/national-critical-functions-overview-508.pdf.

Cyentia Institute. (2023). *Cyentia Cybersecurity Research Library*. https://library.cyentia.com/.

Cyentia Institute. (2020). *IRIS Tsunami: Following the wake of damage from major multi-party cyber incidents*. https://www.cyentia.com/wp-content/uploads/IRIS-Tsunami.pdf.

DBRS Morningstar. (2022). *Global Methodology for Rating Sovereign Governments*. https://www.dbrsmorningstar.com/research/401817/global-methodology-for-rating-sovereign-governments.

De Moor, L., Luitel, P., Sercu, P., Vanpée, R. (2018). Subjectivity in sovereign credit ratings. *Journal of Banking & Finance*, 88, 366-392.

Elezi, E., Gholami, N. (2022). *Albania blames Iran for cyberattacks*. https://www.dw.com/en/albania-once-again-the-target-of-cyberattacks-after-cutting-diplomatic-ties-with-iran-and-expelling-diplomats/a-63146285.

EY. (2022). *How cyber governance and disclosures are closing gaps in 2022*. https://assets.ey.com/content/dam/ey-sites/ey-com/en_us/topics/board-matters/ey-how-cyber-gov-and-disclosures-are-closing-gaps-in-2022.pdf?download.

Federal Bureau of Investigation. (2022). *Ransomware Attacks Straining Local US Governments and Public Services*. (Private Industry Notification No. 20220330-001). https://www.ic3.gov/Media/News/2022/220330.pdf.

Fitch Ratings. (2022). *Sovereign Rating Criteria*. https://www.fitchratings.com/research/sovereigns/sovereign-rating-criteria-11-07-2022.

Fuchs, A., Gehring, K. (2017). The Home Bias in Sovereign Ratings. *Journal of the European Economic Association*, 15(6), 1386-1423.

Ganin, A.A., Quach, P., Panwar, M., Collier, Z.A., Keisler, J.M., Marchese, D., Linkov, I. (2020). Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management, *Risk Analysis*, 40(1), 183-199.

Global Cyber Security Capacity Centre. (2021). *Cybersecurity Capacity Maturity Model for Nations (CMM)*. https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf.

Goodwin, B. (2020). *Cyber gangsters demand payment from Travelex after 'Sodinokibi' attack*. https://www.computerweekly.com/news/252476283/Cyber-gangsters-demand-payment-from-Travelex-after-Sodinokibi-attack.

Government Accountability Office. (2007). *Multiple Efforts to Secure Control Systems are Under Way, but Challenges Remain*. (GAO Publication No. 07-1036). Washington, DC: U.S. Government Printing Office.

Government Accountability Office. (2006). *DHS Leadership Needed to Enhance Cybersecurity*. (GAO Publication No. 06-1087T). Washington, DC: U.S. Government Printing Office.

Government Accountability Office. (2005). *Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities*. (GAO Publication No. 05-434). Washington, DC: U.S. Government Printing Office.

Government Accountability Office. (2004). *Cybersecurity for Critical Infrastructure Protection*. (GAO Publication No. 04-321). Washington, DC: U.S. Government Printing Office.

Greenberg, A. (2018). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Grunert, J., Norden, L., Weber, M. (2005). The role of non-financial factors in internal credit ratings. *Journal of Banking & Finance*, 29(2), 509-531.

Hemsley, K.E., Fisher, R.E. (2018). *History of Industrial Control System Cyber Incidents*. (Publication No. INL/CON-18-44411-Rev002). Idaho Falls, ID: Idaho National Lab.

Hiscox. (2022). *Cyber Readiness Report 2022*. https://www.hiscox.com/documents/Hiscox-Cyber-Readiness-Report-2022.pdf.

HR Ratings. (2017). *Sovereign Debt Methodology*. https://www.hrratings.com/docs/metodologia/0Sovereign%20Debt%20Methodology.pdf.

Hussain, N.Z., Ridley, K. (2020). *Travelex staff go back to basics as ransomware cripples systems*. https://www.reuters.com/article/uk-britain-travelex-idUKKBN1Z70WJ.

Information Week. (2003). *Computer Virus Brings Down Train Signals*. https://www.informationweek.com/it-life/computer-virus-brings-down-train-signals.

ISC2. (2022). *Cybersecurity Workforce Study*. https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx.

Japan Credit Rating Agency. (2021). *Sovereign and Public Sector Entities*. https://www.jcr.co.jp/en/rrinfo/meth_sovereign/.

Japan Credit Rating Agency. (2014). *Types of Credit Ratings and Definitions of Rating Symbols*. https://www.jcr.co.jp/en/pdf/dm24/Rating_Definition20140106.pdf.

Jercich, K. (2020). *'Significant' cyberattack targets UVM health network in Vermont, northern New York*. https://www.healthcareitnews.com/news/significant-cyber-attack-targets-uvm-health-network-vermont-northern-new-york.

Kerner, S.M. (2022). *Colonial Pipeline hack explained: Everything you need to know*. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know.

Kochovski, A. (2023). *The Top 25 VPN Statistics, Facts & Trends for 2023*. https://www.cloudwards.net/vpn-statistics/.

Kovacs, E. (2022). *Cyberattack Causes Trains to Stop in Denmark*. https://www.securityweek.com/cyberattack-causes-trains-stop-denmark/.

Krajnc, D., Glavic, P. (2005). A Model for Integrated Assessment of Sustainable Development. *Resources, Conservation and Recycling*, 43(2), 189-208.

Kroll Bond Rating Agency. (2022). *Understanding Ratings*. https://www.kbra.com/understanding-ratings/rating-scales/long-term-credit-rating.

Kroll Bond Rating Agency. (2021). *Sovereigns Rating Methodology*. https://www.kbra.com/understanding-ratings/methodologies/sovereigns/in-use.

Luitel, P., Vanpée, R., De Moor, L. (2016). Pernicious effects: How the credit rating agencies disadvantage emerging markets. *Research in International Business and Finance*, 38, 286-298.

Marsh McLennan. (2023). *Using data to prioritize cybersecurity investments*. https://www.marsh.com/us/services/cyber-risk/insights/using-cybersecurity-analytics-to-prioritize-cybersecurity-investments.html.

Martin, D. (2016). *Russian hack almost brought the U.S. military to its knees*. https://www.cbsnews.com/news/russian-hack-almost-brought-the-u-s-military-to-its-knees/.

Mellios, C., Paget-Blanc, E. (2006). Which factors determine sovereign credit ratings? *The European Journal of Finance*, 12(4), 361-377.

Montalbano, E. (2021). *Massive DDoS Attack Disrupts Belgium Parliament*. https://threatpost.com/ddos-disrupts-belgium/165911/.

Mulder, C., Perrelli, R. (2001). *Foreign Currency Credit Ratings for Emerging Market Economies*. International Monetary Fund Working Paper No. 01/191.

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Pamment, J., Sazonov, V., Granelli, F., Aday, S., Andžāns, M., Bērziņa-Čerenkova, U., Gravelines, J.P., Hills, M., Holmstrom, M., Klus, A., Martinez-Sanchez, I., Mattiisen, M., Molder, H., Morakabati, Y., Sari, A., Simons, G., Terra, J. (2019). *Hybrid Threats: 2007 cyber attacks on Estonia*. https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86.

Parfomak, P.W., Jaikaran, C. (2021). *Pipeline Cybersecurity: Federal Programs*. (CRS Report No. R46903). https://crsreports.congress.gov/product/pdf/R/R46903.

Parfomak, P.W. (2012). *Pipeline Cybersecurity: Federal Policy*. (CRS Report No. R42660). https://crsreports.congress.gov/product/pdf/R/R42660.

Pearson, J. (2022). *Shell re-routes oil supplies after cyberattack on German firm*. https://www.reuters.com/business/energy/shell-re-routes-oil-supplies-after-cyberattack-german-logistics-firm-2022-02-01/.

Pendleton, M., Garcia-Lebron, R., Cho, J.H., Xu, S. (2016). A Survey on Systems Security Metrics. *ACM Computing Surveys*, 49(4), 1-35.

PwC. (2021). Conti cyber attack on the HSE: Independent Post Incident Review. https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf.

RiskRecon. (2020). *Introducing the updated RiskRecon Cybersecurity Risk Rating Model.* https://www.riskrecon.com/cybersecurity-risk-rating-model.

Roberts, P. (2011). *Carbon Trading Halted After Hack of Exchange.* https://threatpost.com/carbon-trading-halted-after-hack-exchange-012011/74862/.

Romanosky, S., Ablon, L., Kuehn, A., Jones, T. (2019). Content analysis of cyber insurance policies: how to carriers price cyber risk? *Journal of Cybersecurity*, 5(1).

Ruan, K. (2017). Introducing cybernomics: A unifying economic framework for measuring cyber risk. *Computers & Security*, 65, 77-89.

Scope Ratings. (2022). *Sovereign Rating Methodology*. https://scoperatings.com/governance-and-policies/rating-governance/methodologies.

Shameli-Sendi, A., Aghababaei-Barzegar, R., Cheriet, M. (2016). Taxonomy of Information Security Risk Assessment (ISRA). *Computers & Security*, 57, 14-30.

Sohval, B. (2020). *A Deep Dive in Scoring Methodology*. https://securityscorecard.com/resources/deep-dive-scoring-methodology.

Stupp, C. (2021). *Energy Tech Firm Hit in Ransomware Attack*. https://www.wsj.com/articles/energy-tech-firm-hit-in-ransomware-attack-11620764034.

Svítil, M. (2018). The Use of Qualitative Indicators in Banking Rating Systems. *Financial Assets and Investing*, 9(2).

Swinhoe, D. (2019). *Rebuilding after NotPetya: How Maersk moved forward.* https://www.csoonline.com/article/3444620/rebuilding-after-notpetya-how-maersk-moved-forward.html.

S&P Global Ratings. (2022). *Sovereign Rating Methodology.* https://disclosure.spglobal.com/ratings/en/regulatory/article/-/view/sourceId/10221157.

S&P Global Ratings. (2021). *S&P Global Ratings Definitions.* https://disclosure.spglobal.com/ratings/en/regulatory/article/-/view/sourceId/504352.

United Nations International Telecommunication Union. (2015). *Global Cybersecurity Index & Cyberwellness Profiles*. https://www.itu.int/pub/D-STR-SECU-2015.

U.S. Department of Justice. (2002). *British National Charged with Hacking Into N.J. Naval Weapons Station Computers, Disabling Network After Sept. 11.* https://www.justice.gov/archive/criminal/cybercrime/press-releases/2002/mckinnonIndict2.htm.

Verizon. (2022). *Data Breach Investigations Report*. https://www.verizon.com/business/resources/T425/reports/dbir/2022-data-breach-investigations-report-dbir.pdf.

Welburn, J.W., Strong, A. (2021). Systemic Cyber Risk and Aggregate Impacts. *Risk Analysis*, 42(8), 1606-1622.

Whitehead, D.E., Owens, K., Gammel, D., Smith, J. (2017). Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. *70th Annual Conference for Protective Relay Engineers* (pp. 1-8). College Station, Texas, United States: IEEE.

DISTRIBUTION

Email—Internal

Name	Org.	Sandia Email Address
Kevin Griffith	8718	kgriff@sandia.gov
Asmeret Naugle	5522	abier@sandia.gov
Hayden T. Fears	8714	htfears@sandia.gov
Danielle R. Jacobs	8765	djacob@sandia.gov
Megan Nyre-Yu	8741	mnyreyu@sandia.gov
Joshua T. Dise	8714	jtdise@sandia.gov
Ashley Stapp	8714	amstapp@sandia.gov
Nathan Clough	8714	nclough@sandia.gov
Technical Library	1911	sanddocs@sandia.gov

Email—External

Name	Company Email Address	Company Name
Nicholas Winstead	nick@zra.com	ZRA
John Arterbury	john@zra.com	ZRA

This page left blank

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.