Measurability: Toward Proactive Scalable Cybersecurity Management of Large National Infrastructure – USA Healthcare

William Yurcik†
Centers for Medicare & Medicaid Services (CMS)
Baltimore, MD USA
william.yurcik@cms.hhs.gov

Stephen North
Infovisible
Oldwick, NJ USA
scnorth@gmail.com

Rhonda O'Kane
BitSight Technologies
Boston, MA USA
rhonda.okane@bitsighttech.com

O. Sami Saydjari
Dartmouth College
Hanover, NH USA
sami.saydjari@dartmouth.edu

Fabio Roberto de Miranda
Rodolfo da Silva Avelino
Insper Institute of Education and Research
São Paulo, Brazil
{fabiomiranda, rodolfosa1}@insper.edu.br

Gregory Pluta
University of Illinois
Urbana-Champaign, USA
gpluta@illinois.edu

***Abstract*— The current state of cybersecurity protection is reactive response to solving problems as they arise. Many efforts have been undertaken to raise cybersecurity protection awareness and legal liability in an effort to reduce the number and impact of problems, however, problems continue to arise and the result of these improvement efforts is unmeasured and unknown. We propose a new paradigm where cybersecurity posture can be proactively baselined (on a large scale) and then strategic interventions to improve cybersecurity posture can be measured with quantitative results (on a large scale). To demonstrate, we focus on USA healthcare which is currently estimated to be about 17% of the U.S. economy. We show the cybersecurity posture of a large critical national infrastructure can be quantitatively baselined. We accomplish this with an implementation combining the use of data reducing ratings and data visualization techniques. To our knowledge this new paradigm results in the first Internet security management findings for a large national infrastructure.**

Keywords: critical infrastructures protection; cybersecurity quantification; cybersecurity management; hospital cybersecurity.

I. INTRODUCTION

Cybersecurity management encompasses all the planning, implementation, operations, incident response, and remediation required to protect networked resources and ultimately data within an enterprise. Cybersecurity management techniques vary based on the unique enterprise environment and the skills and experience of the people responsible for it.

One powerful management technique that can be employed in the security management domain is the use of quantitative measurement to provide mathematical analysis that are objective, replicable, and enable meaningful precise comparisons [1]. Two influential management theorists, Peter Drucker and W. Edwards Deming, have been falsely attributed with the phrase "If you can't measure it then you can't manage it". This misattribution is understandable since it mirrors both their work. Demings is recognized as the father of total quality management based on continuous measured improvement [2].

However, the use of quantitative measurement for security management is fundamentally challenging for the issues also illuminated by Drucker and Demings- What is important to be managed? What can be measured? Are measurements available for things important to be managed? Can measurements be created for important things to be managed that are currently unmeasured? Can we measure efficiently? We want to measure things important to be managed, not just where measurements are available. What gets measured may get managed even if what we want to manage is not always measurable. Drucker commented directly on this dilemma – "*What gets measured gets managed – even when it's pointless to measure and manage it, and even if it harms the purpose of the organization to do so"* [3].

The current state of cybersecurity management is reactive solving problems as they arise. Cybersecurity & Infrastructure Security Agency (CISA) security management mandated for U.S. Federal agencies consists of enterprise dashboards for critical infrastructures showing system vulnerabilities that have been identified but unpatched and/or otherwise not yet remediated [4]. Log-based security management (e.g., Splunk) and SIEM-based security management (Security Information & Event Management e.g., product RSA NetWitness) consist of enterprise dashboards of prioritized alarms. Compliance-based security management (e.g., Federal Information Security

† Corresponding Author; Official Organizational Disclaimer: "The views presented herein do not represent the views of the Federal Government."

Modernization Act FISMA controls) use an audit control checklist in comparison with a security standard (e.g. NIST 800-53), however, audit controls are not weighted such that one documentation finding is the same as one unimplemented technical control finding leading to the characterization of "check-the-box". Lastly, outsourcing security management to an external entity only transfers responsibility to contractual agreements.

Drucker did actually state, "*The best way to predict the future is to create it"* [3]. In the case of security management, predicting the future is *proactively* creating resilience against future unknown cyberattacks - as opposed to focusing entirely on reactively remediating past known cyberattacks.

We propose a new security management paradigm where cybersecurity posture can be proactively baselined (on a large scale) and then strategic interventions to improve cybersecurity posture can be measured with quantitative results (on a large scale).

To further unpack scalability at a large scale, even if able to produce quantitative security measurements, and given automation support, the volume of security metric information at some point will become too large for human decision-making to take into account relationships, interactions, and emergent properties when making strategic security decisions.

There are two general techniques that can be leveraged to help address scalability. First, numerical data reduction techniques can combine multiple data measurements from multiple sources while retaining underlying information. Second, humans have extraordinary visual processing capabilities, especially for pattern recognition changes, capabilities estimated to be about 10 Mbps with brain reaction times on the order of 150ms [5] [6].

In order to achieve scalable security management, we converged on a two-stage approach consisting of (1) numerical data reduction techniques to reduce data volume and (2) data visualization techniques designed to present information to human decision-makers. After initial proof-of-concept experiments and in-house trial-and-error adjustments, we implemented this two-stage approach for a complex real-world environment.

The remainder of this paper is structured as follows. In Section II, we describe how cybersecurity ratings are derived from empirical security metric measurements. In Section III, we use cybersecurity ratings to baseline large and defined U.S. hospital systems. We end with a summary in Section IV.

II. CYBERSECURITY RATINGS

Cybersecurity ratings based on security metrics can be viewed as a numerical data reduction technique for security metrics, directly analogous to how a credit score is used to encompass overall credit risk by a creditor, and similar to how the current price of a stock or bond encompasses corporate financial reports and market conditions [7].

BitSight invented the ratings industry by creating a transparent algorithm based on security metrics to produce quantitative security scores (ranging from 200-900) for systems/organizations. BitSight is unique in that it incorporates large-scale analysis based on Internet traffic gathered outside of an organization's security perimeter (not egress/ingress traffic) in addition to low frequency network and port scans and open source information.

The previous intuitive analogies we used for cybersecurity rating scores have become physically manifest in the real-world when one of the two largest financial credit rating companies in the world (Moody's) bought an equity stake in BitSight. On 9/13/2021 Businesswire announced Moody's Corporation (New York Stock Exchange NYSE symbol: MCO) invested $250M in BitSight and BitSight acquired VisibleRisk, a cyber risk ratings joint venture created by Moody's and Team8, a global venture group.

Figure 1 shows the security metrics and corresponding weights BitSight uses to calculate their ratings. BitSight groups these security metrics (aka risk vectors) into four categories: (1) Diligence, (2) Compromised Systems, (3) User Behavior, and (4) Public Disclosures. The largest weight is the Diligence risk vector (70.5%) which measures 11 different metrics for best practice implementation. The 4 additional metrics listed under Diligence are currently in beta and do not affect ratings. The next largest weight is the Compromised Systems risk vector (27%) which measures 5 different metrics for evidence of preventing (or lacking to prevent) malicious or unwanted software. The smallest weight is the User Behavior (2.5%) risk vector which measures 3 different activity metrics (open ports, password re-use, and file sharing traffic). Unlike the other three risk vectors, the absence of a Public Disclosure in open source reports does not positively boost ratings but the report of compromise or breach will have a negative impact on ratings.

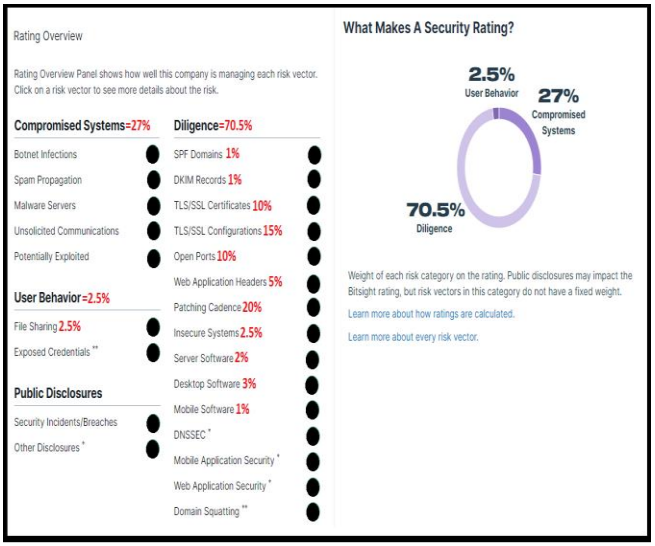

Figure 1. BitSight 2023 Rating Algorithm (used with permission).

For trust and transparency, BitSight publishes its ratings algorithm and annually makes revisions (security metrics and corresponding weights) given user input, changes in the Internet threat environment, and security metric measurement improvements. This follows the well-established model used by other ratings organizations in securities and insurance.

As significant as it is to incorporate an overall cybersecurity risk assessment into one number, a BitSight rating is still only a single data point in time. For human decision-making it is often more important to know where a rating is trending in time as opposed to where it currently stands at the moment. BitSight provides ratings trend sparklines for a one year time period.

Figure 2 is an example BitSight rating trend sparkline annotated with notes documenting rating inflection points. The shaded horizontal rectangle is the expected ratings range where organizations of the same type should be operating. Trends over time are the dominant metric in all ratings organizations especially securities, credit, and insurance. In fact, the Wall Street Journal publishes not only stock prices but individual stock sparklines as demanded by their customers so (as the adage goes) investors and speculators desire to "buy low and sell high".

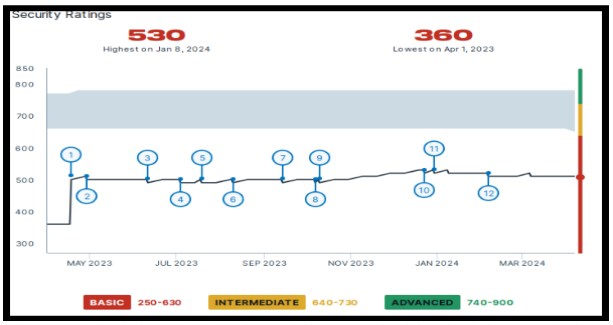

Figure 2. BitSight Annotated Sparkline (used with BitSight permission).

III. BASELINING CYBERSECURITY OF USA HEALTHCARE

At this point, we will pivot to demonstrate how ratings can be used to perform security management on actual infrastructures larger in size than previously possible. Out of possible application domains, we have selected to assess the overall security posture of the USA healthcare sector.

Healthcare includes all organizations, people, and actions whose primary intent is to promote, restore, and/or maintain health. This includes medical providers (doctors/dentists/mental-health-professionals), out-patient urgent care, community clinics, nursing homes, specialized medical equipment providers, health insurers, the pharmaceutical industry, and different types of hospitals.

USA healthcare covers a current population of 333M people, with private group insurance plans covering about 66% of the population, Medicaid covering 89M, Medicare covering 64.5M, the Affordable Care Act covering 21M, and 26M people with no health insurance [8]. As of May 2022 exactly 64,553,288 people were enrolled in Medicare and exactly 88,978,791 people were enrolled in Medicaid and Children's Health Insurance Program (CHIP) [8]. About 12M individuals are dually eligible for both Medicare and Medicaid, so are counted in the enrollment figures for both programs [8]. In January 2024 the Affordable Care Act's Health Insurance Marketplace reached 21M for the 2024 plan year [8]. In September 2023, the U.S. Census reported that for 2022 the number of uninsured U.S. citizens reached a record low of 26M or 7.9% [8]. Note that, due to significant overlaps in coverage, these numbers do not add to the current USA population for the year of study [8]. In 2022, USA healthcare expenditure accounted for $4.5 trillion which is 17.3% of the U.S. Gross Domestic Product (GDP) [8].

To tangibly assess the security posture of USA healthcare, we converged on hospitals as the central point touching every part of the industry – most providers have hospital privileges and hospitals are typically the parent organization of subsidiary activity such as associated out-patient services/facilities. We used multiple open source authorities to assemble a database of 7,490 USA hospitals hosted at the University of Illinois which has been vetted multiple times. Figure 3 shows all USA hospitals mapped to their geographical coordinates in the continental USA.

According to the American Hospital Association, a hospital is state-licensed institution whose function is to provide diagnostic and therapeutic patient services for medical conditions, with organized physician staff and registered nurses. The functional hospitals we are tracking include general hospitals, Short-Term Acute Care Hospitals (STACH), Long-Term Acute Care Hospitals (LTACH), Inpatient Rehabilitation Facilities (IRF), Skilled Nursing

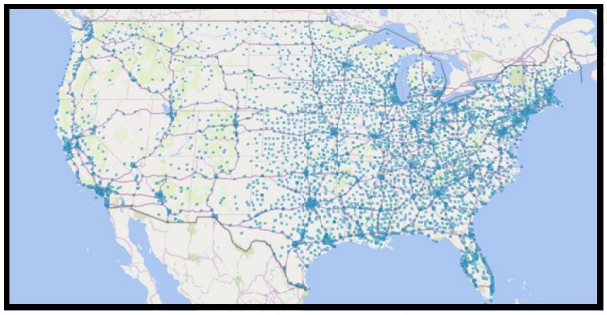

Figure 3. USA Hospitals Geographical Placement.

Facilities (SNF), short stay hospitals, behavioral hospitals, psychiatric care hospitals, children's hospitals, women's hospitals, teaching hospitals, and specialty care hospitals (cancer care, eye surgery, etc). Formal categories of hospitals include Acute Care/Critical Access Hospitals (ACH, fewer than 25 in-patient beds and greater than 35 miles from the next nearest hospital) and Safety-Net Hospitals (designated by the proportion of charity care provided). In addition to leveraging authoritative sources, we identified and vetted hospitals based on healthcare facilities containing in-patient beds, the word "hospital" in their title (which is regulated by state authorities), and Internet website presence.

We subdivided USA hospitals into five separate systems for analysis: (1) Indian Health Service Hospitals, (2) Veterans Health Administration Hospitals, (3) Defense Health Agency Hospitals, (4) Interstate Hospital Systems, and (5) Intrastate Hospital Systems. These five hospital systems include 69% of all the hospitals in the USA, with the remaining hospitals being independent unaffiliated hospitals.

A. Baseline – Indian Health Service (IHS)

IHS is the primary Federal healthcare provider (administered by the U.S. Department of Health & Human Services) for Federally-recognized American Indian tribes and Alaskan natives consisting of approximately 2.6 million people belonging to 574 tribes in 37 states. In the role of primary healthcare provider, IHS provides a comprehensive health service delivery system consisting of 24 IHS hospitals and 22 Tribal hospitals; 51 IHS Health Centers and 279 Tribal Health Centers; and 59 Alaska Village Clinics.

From this IHS/Tribal facility mix, we identified and processed 46 in-patient hospital/medical center facilities located in ten different states containing a cumulative total of 1,620 beds. Of the 46 in-patient facilities, five IHS and nine Tribal Hospitals are critical access hospitals, and one of the Tribal Hospitals is an inpatient rehabilitation facility. Figure 4 shows all IHS hospitals mapped to their geographical coordinates in the continental USA. There are 7 IHS hospitals in Alaska not shown in Figure 4.

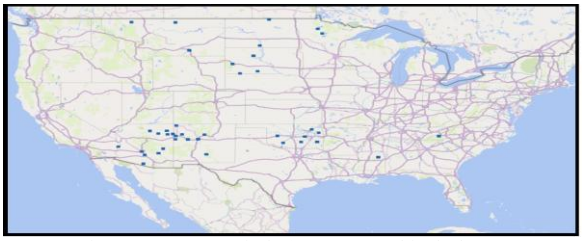

Figure 4. IHS Hospitals (46) Geographical Placement.

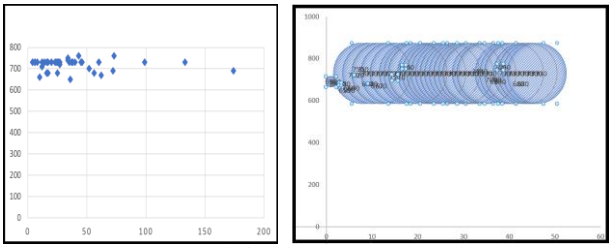

Figure 5. IHS Hospital Ratings (46) vs Hospital Size.

The BitSight rating for each of the 46 in-patient IHS/Tribal facilities are shown in Figure 5 as a function of hospital size. Rightmost Figure 5 is a representation of the number of assets (URLs, IP addresses, domain names) being monitored at each IHS hospital – the more assets the larger the dot/circle. Figure 6 breaks out BitSight ratings and hospital sizes in separate histograms.

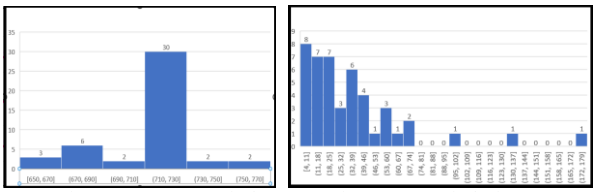

Figure 6. IHS Hospitals (46) Ratings vs Hospital Size.

Leftmost Figure 6 frequency distribution shows the IHS hospital rating scores bundled into histogram bins sizes of 20. The vertical axis is frequency. The IHS hospital system mean rating score is 719.78 with scores ranging from 650-760 (110 range), median/mode of 730, a negative skew of -1.23 (median/mode higher than mean) with more scores higher than the mean, and a 95% confidence interval around the mean of 712.53 - 727.03. Twelve IHS hospitals fall outside-below the mean 95% confidence interval.

The rightmost Figure 6 histogram shows the distribution of IHS hospital sizes as measured by in-patient beds in bins sizes of 7 beds. While the mean size of an IHS hospital is 36 in-patient beds, almost half of the IHS hospitals are smaller critical access hospitals defined as being less than or than or equal to 25 in-patient beds.

B. Baseline - U.S. Veterans Health Administration (VHA)

VHA is the largest healthcare system in the world providing healthcare for about 9 million non-active/discharged veterans of the U.S. military annually at 1,321 healthcare facilities, including 172 medical centers, 1,138 community-based outpatient clinics, and 134 Community Living Centers (e.g. nursing homes) [9]. All VHA healthcare facilities are owned and operated by the U.S. Department of Veteran Affairs and the approximate 350,000 VHA healthcare staff are Federal employees making them the second largest workforce cohort in the U.S. government [9] [10]. Multiple reports show VHA hospitals provide quality healthcare that is equal to, and often better than, healthcare provided by private sector hospitals [11] [12].

Figure 7. VHA Hospitals (168) Geographical Placement.

We processed 168 in-patient VHA hospital/medical center facilities located in 51 states (including Washington D.C.) containing a cumulative total of 38,296 beds. Figure 7 shows all VHA hospitals mapped to their geographical coordinates. Not shown in Figure 7 are VHA hospitals in Alaska(1), Hawaii(1), and Puerto Rico(1).

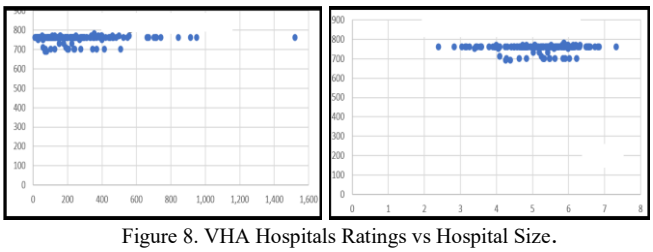

Figure 8. VHA Hospitals Ratings vs Hospital Size.

Figure 8 shows a scatter plot of ratings for VHA hospitals. The vertical axis is ratings and the horizontal axis is the number of in-patient beds within each of the 168 VHA hospitals (leftmost horizontal axis is straight scale, rightmost horizontal axis is scaled log base e). Figure 9 breaks out the

ratings and hospital sizes for VHA hospitals into separate frequency distribution histograms.

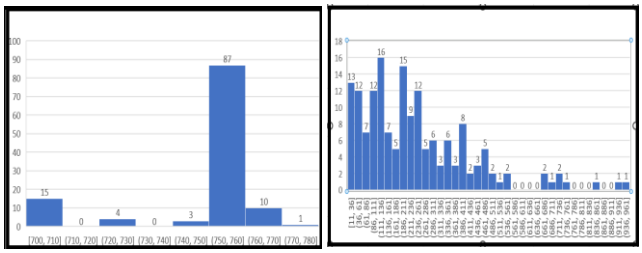

Figure 9. VHA Hospitals (168) Ratings & Hospital Size.

The leftmost Figure 9 frequency distribution shows the VHA hospital ratings bundled into histogram bins sizes of 10. The vertical axis is frequency. The VHA hospital system mean rating score is 753.78 with scores ranging from 690-780 (90 range), median/mode of 760, a negative skew of -2.27 (median/mode higher than mean) with more scores higher than the mean, and a 95% confidence interval around the mean of 750.81 – 756.74. Twenty-five VHA hospitals fall outside-below the 95% confidence interval for the mean.

The rightmost Figure 9 indicates VHA hospital sizes via a frequency distribution histogram of in-patient hospital beds with a bin size equal to 25. The mean size of a VHA hospital is 248.18 in-patient beds. The large Chillicothe VHA Medical Center in Ohio with 1,522 in-patient hospital beds is included in mean in-patient bed calculation but intentionally omitted in Figure 9 display for data visibility.

C. *Baseline - U.S. Defense Health Agency (DHA)*

DHA is operated by the U.S. Department of Defense as the healthcare provider for active-duty members of the U.S. military with hospitals and clinics worldwide. About 9.4M active-duty members of the U.S. military use DHA hospitals and clinics with TRICARE military health insurance expenditures representing about 8% of the U.S. Department of Defense (DoD) budget [13].

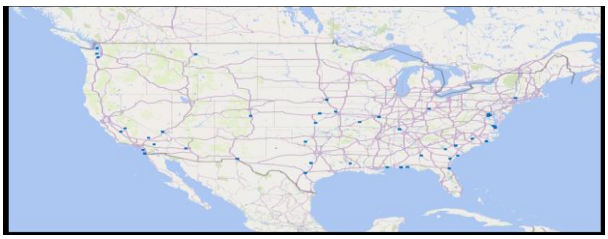

Figure 10. DHA Hospital (48) Geographical Placement.

For the purposes of this paper we will focus only on DHA hospitals located in the USA. We identified and attempted to process 48 in-patient DHA hospital/medical center facilities located in 25 states containing a cumulative total of 8,358 beds. Figure 10 shows all DHA hospitals mapped to their geographical coordinates in the continental USA. Not shown in Figure 10 are DHA hospitals in Alaska(2) and Hawaii(1).

Figure 11 indicates the distribution of DHA hospital sizes with a frequency distribution histogram of in-patient hospital beds with bin size equal to 25. The mean size of a DHA hospital is 181.70 in-patient beds. The large Blanchfield Army Community DHA Hospital at Fort Campbell in Kentucky with 2,100 in-patient hospital beds is included in mean in-patient bed calculation but intentionally omitted from Figure 12 display for data visibility.

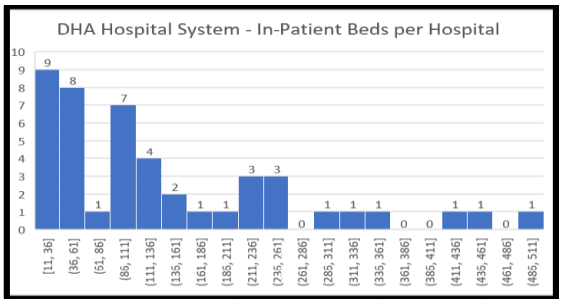

Figure 11. DHA Hospitals (48) – Hospital Size Distribution.

We found the ratings for each of the 48 in-patient DHA Hospitals was pegged at 770 (no variation) and the number of assets detected at each DHA hospital was also pegged at 28 (no variation). DHA facilities are located on secure military installations and all DHA hospitals and clinics are networked together by nine Defense Health Networks which are "dual-hatted" accountable to both DHA and military commands. Given this classified national security environment it is to be expected our attempts to derive ratings were only partially successful with incomplete results.

D. *Baseline – Interstate Hospital Systems*

USA hospitals are increasingly combining into systems of multiple hospitals sharing the same IT infrastructure – for reasons beyond the scope of this paper. We subdivided these hospitals systems into two categories for analysis: (1) Interstate Hospitals Systems containing hospitals in multiple states and (2) Intrastate Hospital Systems containing hospitals all within one state. This separation based on state boundaries is meaningful since hospital administration is generally governed by state regulations/certifications/laws.

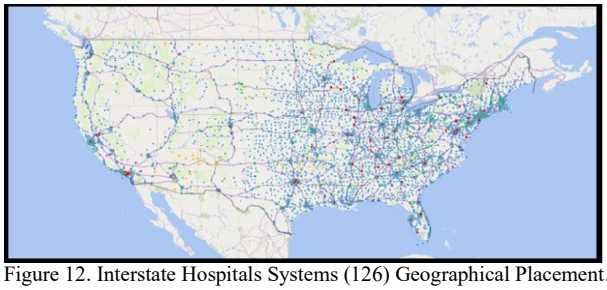

Figure 12. Interstate Hospitals Systems (126) Geographical Placement.

Figure 12 shows the headquarters location of all USA Interstate Hospital Systems mapped to their geographical coordinates in the continental USA. No Interstate Hospital Systems are headquartered in Alaska or Hawaii. We identified 126 Interstate Hospital Systems with a mean size of 21.38 hospitals ranging in size from a two hospital Interstate Hospital System (4 systems) to 84/127/158 hospital Interstate Hospital Systems (HCA Healthcare/Ascension

Healthcare/Encompass Health Interstate Hospital Systems respectively). We identified Interstate Hospital Systems ranging from across only 2 states (60 systems) to Interstate Hospital Systems ranging across 25/37 states (Select Specialty Hospitals/Encompass Health respectively) with the mean number of states in an Interstate Hospital System equal to 4.96 hospitals.

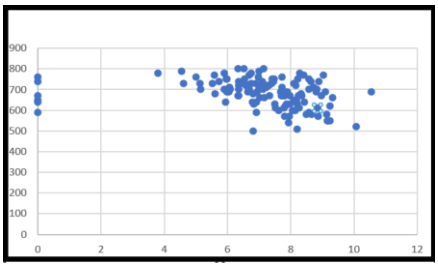

Figure 13. Ratings for Interstate Hospital Systems (126) vs Size.

Figure 13 shows a scatter plot of ratings for USA Interstate Hospital Systems. The rating for each Interstate Hospital System is the combined aggregate score of all hospitals in that system. The vertical axis is ratings and the horizontal axis is the logarithm (base e) of the number of in-patient beds within a hospital.

Figure 14 breaks out ratings and hospital sizes for USA Interstate Hospital Systems into frequency distribution histograms. The leftmost Figure 14 frequency distribution shows the USA Interstate Hospital Systems ratings bundled into histogram bin sizes of 48. The vertical axis is frequency. The USA Interstate Hospital System mean rating is 682.72 with scores ranging from 500 - 800 (300 range), median/mode of 690, a negative skew of -0.52 (median/mode higher than mean) with more scores higher than the mean, and a 95% confidence interval around the mean (684) of 671.00 – 694.72. Fifty USA Interstate Hospital Systems fall outside-below the 95% confidence interval for the mean.

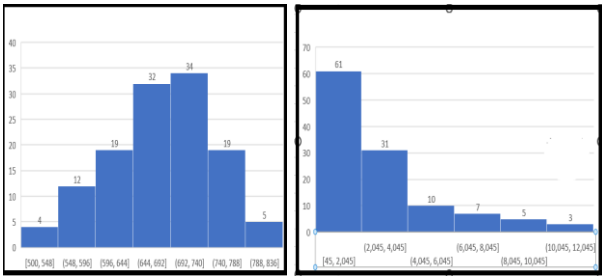

Figure 14. USA Interstate Hospital Systems (126) - Ratings & Hospital Size.

The rightmost Figure 14 indicates USA Interstate Hospital sizes via a frequency distribution histogram of in-patient hospital beds with a bin size equal to 2000. The capacity of in-patient beds within Interstate Hospital Systems range in size from 45 beds (Brightwell Behavioral Health) to 23,557 beds (HCA Healthcare). The mean size of a USA Interstate Hospital System is 3,171.23 in-patient beds, median equal to 1,816 beds and mode equal to 365 beds, with skew equal to 4.76 and stdev equal to 4,598 beds. The large HCA Interstate Health System (23,557 in-patient hospital beds) is included in calculations but intentionally omitted in the Figure 15 display for data visibility.

E. Baseline – IntraState Hospital Systems

With USA state regulations/certifications/laws governing the administration of hospitals, a large number of USA Intrastate Hospital Systems have emerged confined within a single state boundary. We identified 523 Intrastate Hospital Systems across all states ranging in size from two hospitals (167 different Intrastate Hospital systems) to 46 hospitals (Baylor Scott & White Health in Texas) with a mean of 4.92 hospitals. Texas has the largest number of Intrastate Hospitals Systems (41 systems) as well as the most hospitals affiliated within an Intrastate Hospital System (255 hospitals). At the other extreme, Alaska, District of Columbia, and Vermont only have one Intrastate Hospital System, and this one Intrastate Hospital System consists of only one hospital in each of these states.

Figure 15 shows the headquarters location of all USA Intrastate Hospital Systems mapped to their geographical coordinates in the continental USA. Figure 16 shows two scatter plots of BitSight Ratings for USA Intrastate hospital systems. Each Intrastate Hospital System consists of multiple hospitals physically located within the same state and networked together sharing the same IT infrastructure. The rating for each Intrastate Hospital System is the combined aggregate score of all hospitals in that system.

Figure 15. Interstate Hospitals Systems (126) Geographical Placement.

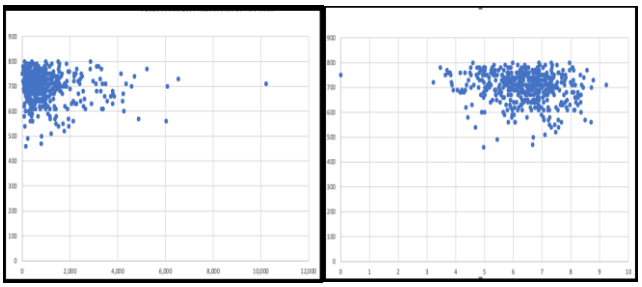

Figure 16. Ratings for Intrastate Systems (523) vs Size.

Figure 16 vertical axis are both ratings, the horizontal axis for the leftmost scatterplot is the number of in-patient beds within a hospital and the horizontal axis for the rightmost scatterplot is the logarithm (base e) of the number of in-patient beds within a hospital. Figure 17 breaks out the

BitSight ratings and hospital sizes for Intrastate Hospital Systems into separate frequency distribution histograms.

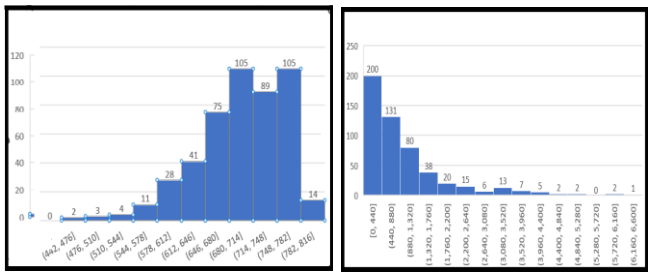

Figure 17. Intrastate Hospital Systems (523) - Ratings and Size.

The leftmost Figure 17 frequency distribution shows the USA Intrastate Hospital Systems security ratings bundled into histogram bins sizes of 34. The vertical axis is frequency. The USA Intrastate Hospital System mean security rating is 699.34 with scores ranging from 460-800 (340 range), median/mode of 710, a negative skew of -0.89 (median/mode higher than mean) with more scores higher than the mean, and a 95% confidence interval around the mean (699.34) of 693.73 – 705.04. Twenty-nine USA Intrastate Hospital Systems fall below the 95% confidence interval for the mean.

The rightmost Figure 17 indicates USA Intrastate Hospital sizes via a frequency distribution histogram of in-patient hospital beds with a bin size equal to 440. The mean size of a USA Intrastate Hospital System as measured in in-patient beds is 955.56 beds (median=626, mode=450, skew=2.95). The capacity for in-patient beds within Intrastate Hospital Systems ranges in size from only 28 beds (Altus Health System in Texas) to 10,214 beds (State of California Health System). New York has the largest number of in-patient beds within an Intrastate Hospital Systems (56,422) while the smallest number of in-patient beds within an Intrastate Hospital Systems is in Vermont (25). The large State of California Hospital System (10,214 in-patient hospital range beds) is included in mean in-patient bed calculation but intentionally omitted in the Figure 17 display for data visibility.

IV. SUMMARY

We have introduced, described, and demonstrated a new cybersecurity rating measurability approach for proactive and scalable security management suitable for infrastructures that are larger in size than previously possible to assess - infrastructures that are national in scale. This new paradigm is based on empirical cybersecurity metric data, and proactive, forward-looking, designed to prevent the next attack rather than focusing on remediating past attacks. For instance, cybersecurity ratings are most sensitive to having time-responsive system patching, and not as sensitive to standardized patching cadences for well-known systems who have regularly been attacked in the past.

Baselining is key to establishing fixed references for measuring progress, managing changes, and assessing performance against schedules and cost. A cybersecurity baseline also provides a reference point for tracking deviations, identifying potential issues, making informed decisions, and ensuring all stakeholders have a unified understanding of goals and expectations.

In this paper we performed proof-of-concept experimental baselining of an actual large national infrastructure (USA hospital systems). Our next step will be to demonstrate how interventions with security investments can be strategically designed to improve security and quantitatively measured for their effectiveness using cybersecurity ratings.

We have also used cybersecurity rating techniques to great effect to investigate other urgent problems. Using cybersecurity ratings again in the USA hospital system context, we discovered three cybersecurity "magnified vulnerabilities" in that a single successful exploit can have an outsized impact on the entire nationwide U.S. healthcare infrastructure [14].

ACKNOWLEDGMENTS

This research was enabled through a cooperative agreement between the University of Illinois at Urbana-Champaign and BitSight. BitSight provided no financial support to this research. Cybersecurity ratings for hospitals presented in this research were processed by BitSight engineers led by Rhonda O'Kane and supported by Tadd Hopkins, Tim Jackson, Tom Linehan, and Will Ricardi. Geocoding was provided by GeoCoder.ca who provided public service access to their geography mapping scripts. Geocoder.ca provided no financial support to this research. Authors Miranda and Avelino were supported by a joint funding support agreement between the Insper Institute of Education & Research and the Computer Science Department at the University of Illinois at Urbana-Champaign.

REFERENCES

[1] National Institute of Standards and Technology (NIST), "Measurement Guide for Information Security: Volume 1 – Identifying and Selecting Measures," NIST SP 800-55, vol. 1. January 17 2024.

[2] M. Best and D. Neuhauser, "W. Edwards Deming: Father of Quality Management, Patient and Composer," Quality and Safety in Health Care, 14(4) Sept 2005. <doi::10.1136/qshc.2005.015289>

[3] P. Drucker, "The Essential Drucker: In One Volume the Best of Sixty Years of Peter Drucker's Essential Writings on Management," Harper Collins Publishers, 2001.

[4] Cybersecurity & Infrastructure Security Agency (CISA), Critical Infrastructure Sectors. retrieved February 9, 2024 from <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors>

[5] K. Koch et al., "How Much the Eye Tells the Brain," Current Biology vol. 16, July 25, 2006. <doi:10.1016/j.cub.2006.05.056>

[6] S. Thorpe, D. Fize, and C. Marlot, "Speed of Processing in the Human Visual System," Nature. vol. 381, July 6, 1996. <doi:10.1038/381520a0>

[7] S. J. Choi and M. E. Johnson, "The Relationship Between Cybersecurity Ratings and the Risk of Hospital Data Breaches," J of the Am Medical Informatics Assoc, 2021.

[8] CMS National Health Expenditures (NHE) Fact Sheet. <https://www.cms.gov/data-research/statistics-trends-and-reports/national-health-expenditure-data/nhe-fact-sheet#>

[9] Veterans Health Administration (VHA). retrieved March 29, 2024. from <https://www.va.gov/HEALTH/>.

[10] Congressional Budget Office, "Quality Initiatives Undertaken by the Veterans Health Administration," CBO Report, August 2009.

[11] S.M. Asch et al., "Comparison of Quality of Care for Patients in the Veterans Health Administration and Patients in a National Sample," Annals of Internal Medicine, 141(12), 2004. <doi:10.7326/0003-4819-141-12-200413310-00010>

[12] A.N. Trivedi, S. Matula, I. Miake-Lye, P.A. Glassman, P. Shekelle, and S. Asch, "System Review: Comparison of the Quality of Medical Care in Veterans Affairs and Non-Veterans Affairs Settings," Medical Care, 49(1) 2011. <doi:10.1097/mir.0b013e3181f53575>

[13] "Health.mil - The Official Website of the Military Health System," retrieved March 29, 2024 from <https://www.health.mil/About-MHS/OASDHA/Defense-Health-Agency/>

[14] W. Yurcik et al., "Cybersecurity Monitoring/Mapping of USA Healthcare (All Hospitals) – Magnified Vulnerability due to Shared IT Infrastructure, Market Concentration, & Geographical Distribution," ACM CCS Workshop on Cybersecurity in Healthcare (HealthSec), 2024. <doi:10.1145/3689942.3694754>