Measurability: Toward Integrating Metrics into Ratings for Scalable Proactive Cybersecurity Management

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, IL USA
gpluta@illinois.edu

***Abstract*— We share our experience implementing cybersecurity metric-based algorithmic ratings to proactively manage the cybersecurity of a large critical national infrastructure - U.S. healthcare. We describe the cybersecurity metrics we use, how cybersecurity ratings are algorithmically produced from these metrics, and empirical evidence for the value of cybersecurity ratings to both benchmark and make comparisons. Specifically, we share examples of how cybersecurity ratings can be used to baseline the cybersecurity posture of large hospital systems and how cybersecurity ratings can be used to calculate Return-On-Investment (ROI).**

Keywords - cybersecurity risk quantification; cybersecurity risk management; cybersecurity investment; cybersecurity metrics.

I. INTRODUCTION

Cybersecurity ratings based on empirical metrics are an attempt to characterize overall cybersecurity posture by integrating multiple cybersecurity aspects that can be measured. Ideally, we would like to derive one number that provides intuitive information about an enterprise cybersecurity posture at a point in time, as well as trends over longer time periods. However, cybersecurity ratings also raise challenges such as:

- *Are cybersecurity ratings measuring the right things?*
- *Are important cybersecurity aspects unmeasurable and/or unquantifiable?*
- *Is an overall cybersecurity rating meaningful, a false sense of cybersecurity, or a mischaracterization of effective cybersecurity practices?*
- *Can cybersecurity ratings be covertly gamed by adversaries to misrepresent results?*

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

As Anderson and Moore stated emphatically in 2006 – "*Risks cannot be managed better until they can be measured better"* [1]. In this paper, we report that nineteen years later that understanding of cybersecurity metrics have matured to the point where risks are now being measured, albeit imperfectly, such that enterprises are able to make decisions based on cybersecurity metrics, processed algorithmically into the form of cybersecurity rating, for improved cybersecurity operations and accountable cybersecurity investments.

The remainder of this paper is structured as follows. In Section II, we make the case for enterprise cybersecurity posture information as vital to enterprise cybersecurity operations. In Section III, we provide background on security metric research. In Section IV, we describe how we derive cybersecurity ratings from empirical security metric measurements. In Section V, we use cybersecurity ratings to perform cybersecurity posture analysis of a large national infrastructure – U.S. healthcare. We end with a summary and conclusions in Section VI.

II. CYBERSECURITY OPERATIONS

Cybersecurity operations encompass a range of functions aimed at protecting an organization's information and systems from cyber threats. These functions include monitoring, detecting, responding to, and recovering from cybersecurity incidents, as well as implementing preventative measures and ensuring compliance. Key areas include maintaining network defense, deploying new cybersecurity solutions, and managing Security Operations Centers (SOCs).

Figure 1 graphically depicts cybersecurity operations in multiple dimensions – we would like to highlight that the "evaluate" stages are reactive and the "direct and monitor" stages are proactive – which is where a cybersecurity operations team should strive to be positioned in order to prevent successful cybersecurity attacks.

In order to operate at the proactive cybersecurity operation stages, information is needed to focus efforts.

Cybersecurity operations leverage information from an organization's enterprise attack surface to improve cybersecurity posture and minimize risk – with the attack surface consisting of all IT assets that are potentially exposed to attackers (public-facing assets), including both known and unknown assets. To do this cybersecurity operations teams probe attack surface assets for vulnerabilities, misconfigurations, and other weaknesses that attackers could exploit, typically using vulnerability scanning and penetration testing. Threat modeling also helps to identify potential attack paths and impacts on business operations.

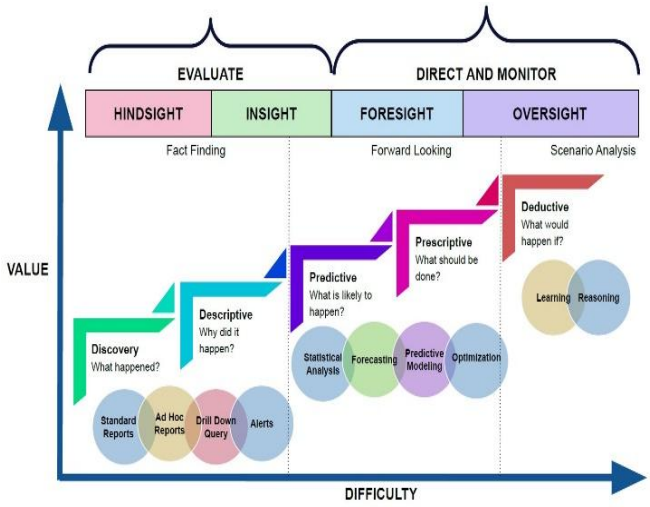

Figure 1. Overview of the Cybersecurity Operations Process.

Figure 2 shows a graphic depiction of the cybersecurity vulnerability cycle - a continuous cyclical process that includes identifying, assessing, prioritizing, remediating, and monitoring vulnerabilities before they can be exploited. Since addressing the number of vulnerabilities and attacks paths to be remediated is a continuous cyclical process, protective actions need to be prioritized based on risk.

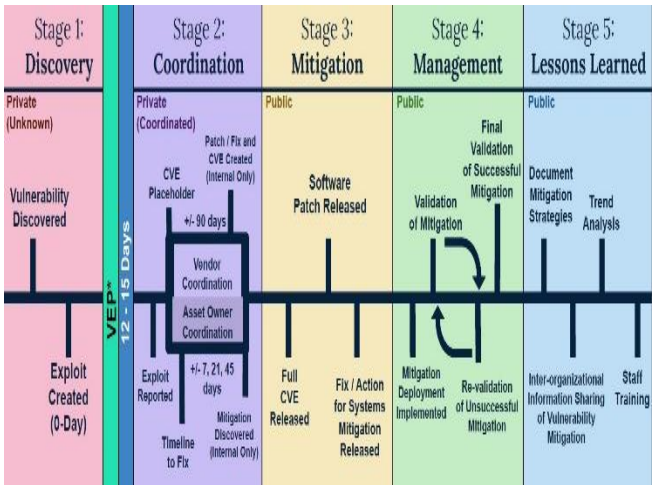

Figure 2. Lifecycle of a Cybersecurity Software Vulnerability.

Figure 3 shows a knowledge gap resulting from two other worrisome effects, the number of undetected attack surface threats is significant and growing over time.

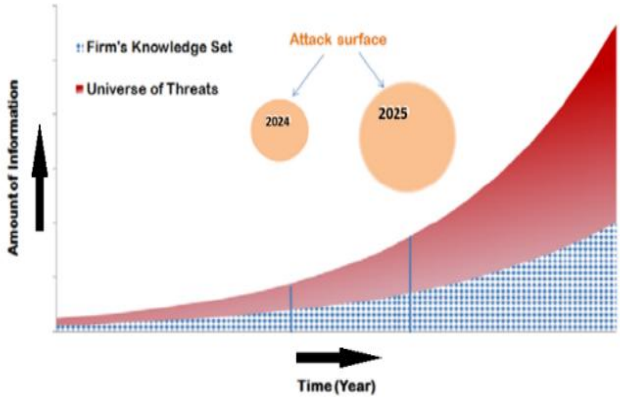

Figure 3. Knowledge Gap with Attack Surface Growth Over Time.

III. CYBERSECURITY METRICS

One of the most frustrating and ultimately dangerous things about cybersecurity is that it can *almost* be measured [2]. Creating an overall cybersecurity posture by measuring various components is complex and currently unsolved [3]. While security metrics can quantify aspects of security, they cannot definitively determine if a system is secure in absolute or relative terms [4].

There continues to be an essential requirement for organizations and engineers to more accurately evaluate overall security posture beyond subjective qualitative assessments. Unfortunately, misinformation and snakeoil are also filling this space. This work aims to quantitatively assess the overall cybersecurity posture, recognizing that it is an approximation. It is our stance that insistence on perfection in the form of a mathematical proof should not prevent implementation of "good enough" improvements over the status quo, especially when a vital need exists.

The U.S. National Institute of Standards and Technology (NIST) defines a metric as a measurement tool that supports human decision-making to enhance cybersecurity performance [5]. Cybersecurity metrics lack a standard best practice, as they are shaped by individual enterprise environments and the staff responsible for implementing cybersecurity operations.

The challenge of identifying cybersecurity metrics persists despite significant efforts over the past two decades. Since June 2000, numerous dedicated forums have addressed this topic, starting with NIST. Below, we present a partial list of major cybersecurity metric forums and highlight key contributions outside these forums [6] - [32].

- NIST Computer System Security and Privacy Advisory Board (CSSPAB) *"Approaches to Measuring Security"*, June 2000.
- *Workshop on Security Metrics (MetriCon)* 2006-2019.

- *International Workshop on Security Measurements and Metrics (MetriSec)* 2010-2012.
- *International Workshop on Quantitative Aspects in Security (QASA*) 2012-2017.

Possible security metrics include quantitative discrete and/or continuous data sources. In Figure 4, we show *proactive* cybersecurity metrics we have used in experimentation. Note these metrics look forward beyond reactive dashboard tracking the remediation of Known Exploited Vulnerabilities (KEVs) and Common Vulnerabilities and Exposures (CVEs) [33][34]. The objective for these cybersecurity metrics is to provide an indication what may happen next, beyond what has already happened in the past.

The cybersecurity metrics in Figure 4 can all be measured and quantified in different ways from *numerical-native* metrics such as incident-response-times and number-of-tested-systems-with-assessments to *categorical string-native* metrics that can be quantified in rankings (different levels of reported exposed credentials) or binary (existence of unapproved applications or not).

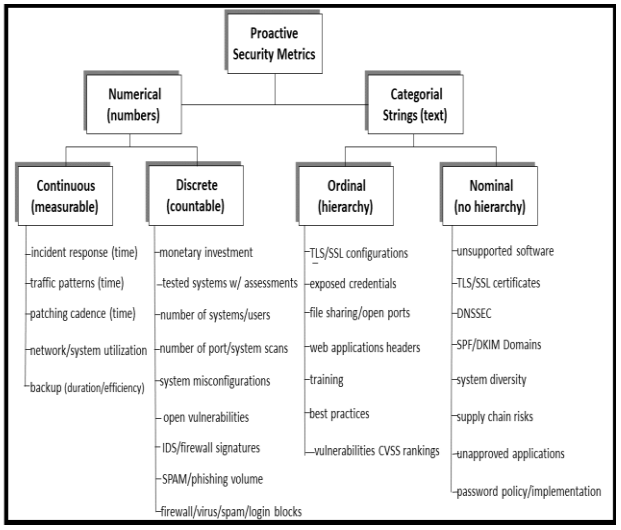

Figure 4. Selected Proactive Cybersecurity Metrics.

For example, about the proactive nature of just two of these cybersecurity metrics, a shorter patching cadence has been documented to be correlated with less risk since it reduces the window of time that a system is vulnerable to a known exploit [35] and implementation of any or all of the following email-related protocols – the Sender Policy Framework (SPF) protocol, the DomainKeys Identified Mail (DKIM) protocol, and the Domain-based Message Authentication, Reporting & Conformance (DMARC) protocol - have proven effective at preventing email spoofing, reducing spam and potential for phishing attacks by verifying legitimacy of email senders [36].

IV. CYBERSECURITY RATINGS

A Cybersecurity Rating is a data-driven dynamic measurement of an organization's cybersecurity performance used to manage enterprise and third-party cyber risk.

In everyday life, assessment ratings systems based on underlying metrics are in ubiquitous use to assess complex systems. Three examples include (1) human physical health, (2) national economies, and (3) financial instruments.

To assess human physical health, doctors use a variety of metrics such as age, weight, sex, heart rate, breathing rate, blood pressure, temperature, waist size, and blood test scores including cholesterol and blood sugar levels. To assess national economies, economists use metrics such as inflation rate, unemployment rates, gross domestic product growth, consumer spending, and gross national income per capita. For financial instruments such as a stock, analysts use price-to-earnings ratio, price-to-sales ratio, earnings per share, debt-to-equity ratio, return on equity, free cash flow, and enterprise value. For each of these examples, the underlying metrics can be combined to provide an overall assessment of physical health, national economic health, and stock price valuation respectively.

Cybersecurity ratings measure security effectiveness and have been validated against actual cybersecurity attacks. One such study positively matched cyberinsurance claims data with cybersecurity ratings showing lower ratings indicate the higher probability of a successful cybersecurity attack [37].

A. Selecting Cybersecurity Metrics

In this same way as these intuitive real-world examples, cybersecurity ratings combine security metrics to a single data point indication of overall cybersecurity assessment. Figure 5 shows 13 cybersecurity metrics that we have utilized as workable inputs to a cybersecurity ratings algorithm.

01	Bitsight Security Rating	08	Web Application Headers
02	Patching Cadence	09	User Behavior
03	Desktop Software	10	TLS/SSL Configurations
04	Potentially Exploited Systems	11	Open Ports
05	Mobile Software	12	TLS/SSL Certificates
06	Botnet Infections	13	Spam Propagation
07	Insecure Systems	14	Unsolicited Communications

Figure 5. Selected Metrics for Cybersecurity Ratings Algorithm.

B. Weighting Cybersecurity Metrics in a Linear Algorithm

The largest weight (70.5%) measures 11 different underlying submetrics for best practice implementation [patching cadence, web application headers, TLS/SSL certificates/configurations]. The next largest weight is an indication of compromised systems (27%) which measures

evidence of preventing (or lacking to prevent) malicious or unwanted software [unsupported software, potentially exploited systems, botnet infection, insecure systems, spam]. The smallest weight is user behavior (2.5%), which measures three different activity metrics [open ports, password re-use, and file sharing traffic].

C. Longitudinal Analysis

A cybersecurity rating is a single data point in time, but its trend over time is more important. Analysts in securities, credit, and insurance industries prioritize these trends to better assess risk. For this reason, we use longitudinal "sparklines" to show the cybersecurity rating varying over a one-year time period. Figure 6 shows a cybersecurity rating sparkline varying over a year with a shaded rectangle indicating the expected "technology industry range" where organizations of the same type should be operating.

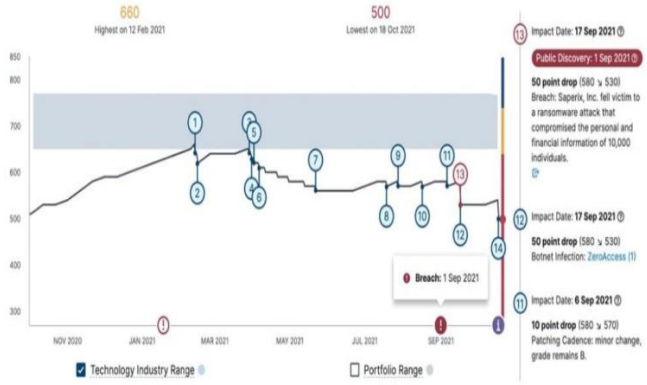

Figure 6. Cybersecurity Rating Sparkline Over a One Year Time Period.

V. Cybersecurity Rating Results

We applied cybersecurity ratings to tangibly assess the cybersecurity posture of USA healthcare. We converged on hospitals as a central point touching every part of healthcare – 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 7 shows all USA hospitals mapped to their geographical continental coordinates.

Hospitals have a broad network attack surface due to their public interactions. Their IT systems manage medical, administrative, financial, and record-keeping operations. Each application and device on the hospital network is a potential entry point for cyberattacks. Therefore, assessing hospital cybersecurity is crucial.

Figure 7. USA Hospitals Mapped to Geographical Coordinates.

Given the critical nature of hospitals, cybercriminals have realized that if they can successfully compromise a hospital enterprise environment using ransomware, then there is a high probability of payment. Hospitals handle Personally Identifiable Information (PII) (including financial data) and Personal Health Information (PHI) that can be monetized in dark web marketplaces. With financial viability at stake and healthcare-related investments being a cost center, hospital investments in cybersecurity protection in terms of staff and equipment are far below other industry levels [38]. Despite this below average investment, hospitals have cybersecurity ratings consistent with other industries, as shown in Figure 8.

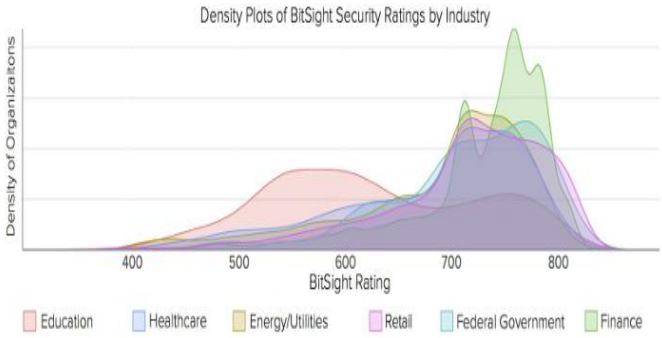

Figure 8. Industry Density Plot of Cybersecurity Ratings (provided by BitSight).

A. Cybersecurity Ratings for Baselines

Baselines provide a starting point for measuring continuous improvement as reflected in higher cybersecurity rating scores. Achieving higher cybersecurity ratings will not happen on its own but requires strategic cybersecurity investments in order to maintain and improve. Without strategic cybersecurity investments over long periods of time, decreased cybersecurity ratings will result as technology advances and existing cybersecurity protection techniques degrade and become obsolete.

Table I provides a comparison of the cybersecurity rating baselines for each of the hospital systems we analyzed. The baselines of the Indian Health Service (IHS) and Veterans Health Administration (VHA) hospital systems are statistically significantly different from each other and statistically significantly different from both Interstate/Intrastate Hospital Systems since their 95% confidence intervals for their means do not overlap. However, the baselines of Interstate/Intrastate Hospital Systems are not statistically significantly different from each other since their 95% confidence intervals for their means do overlap. This makes intuitive sense since both the IHS and VHA Hospital Systems have their own unique centralized IT coordination while Interstate/Intrastate Hospital Systems each consist of many different independent hospital systems, with each hospital system acting independently with little IT coordination between hospital systems.

TABLE I. CYBERSECURITY RATINGS FOR FOUR HOSPITAL SSTEMS.

Security Rating Stats	**IHS**	**VHA**	**INTERSTATE SYSTEMS**	**INTRA-STATE SYSTEMS**
Mean	719.8	753.8	682.7	699.3
95% CI	+/- 7.25	+/- 2.96	+/- 12.00	+/- 5.62
Median	730	760	690	710
Range	650-760 (110)	690-780 (90)	500-800 (300)	460-800 (340)
Skew	-1.23	-2.27	-0.52	-0.89
Targets	12	25	50	29

B. Cybersecurity Ratings for Identifying Interventions

Interventions in cybersecurity protection can be measured with changes in cybersecurity ratings in order to quantify the impact of managing strategic cybersecurity investments. It would be expected that an investment in cybersecurity protection would move the mean cybersecurity rating higher. To claim a positive change from the baseline (with statistical significance) confidence intervals should not overlap.

Larger enterprises typically have lower cybersecurity ratings than smaller enterprises since having more IT assets/systems creates a larger attack surface which is harder to protect. In order to ensure ratings are calculated in a way that does not unfairly bias results based on size, we need to normalize cybersecurity ratings based on organizational size using employee count as a surrogate for size. We acknowledge that this normalization approach of using employee count as an approximation for organizational size may be problematic since organizations vary greatly in their IT complexity.

Even with normalization for size, comparison using a mean cybersecurity rating still treats all hospitals in a hospital system as being equal. We know all hospitals in a hospital system are not equal; when a hospital outage occurs due to a successful ransomware attack some hospitals treat more patients than others (as measured in admittance levels and in-patient beds) and other hospitals are more likely to suffer adverse patient impacts (as measured in mortality). Thus, selecting investments for cybersecurity protection in order to improve the cybersecurity posture of a hospital system becomes a multidimensional optimization problem.

While deriving a multidimensional optimization problem as expressed in a weighted linear equation is beyond the scope of this paper, we can visually illustrate this optimization problem limited to two dimensions, cybersecurity ratings and hospital beds, using the hospital systems we have analyzed.

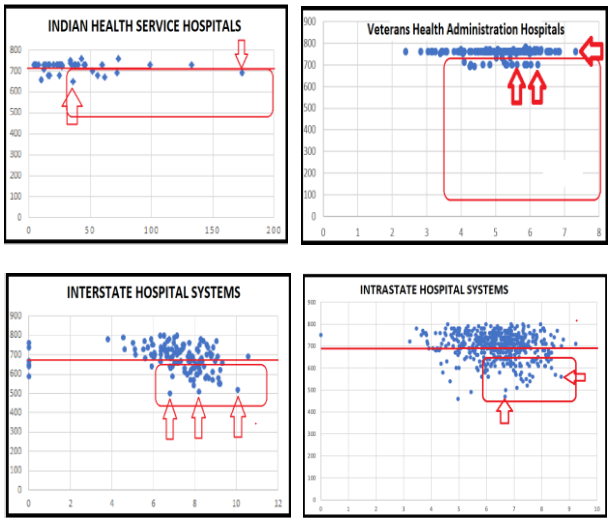

Figure 9. Hospital Targets for Cybersecurity Protection Investment.

Figure 9 shows scatterplots of hospital systems we have analyzed with each scatterplot mapping cybersecurity ratings versus hospital size as measured by in-patient hospital beds. We consider two dimensions for selecting hospitals for investment in cybersecurity protection resulting in the largest beneficial patient outcome and the largest increase in cybersecurity rating score, the largest hospitals with the lowest cybersecurity rating, basically the lower right quadrant. The last row in Table I indicates the number of potential target hospitals/systems which would be the best candidates for cybersecurity protection investment within each hospital system, resulting in a statistically significant increase in cybersecurity rating.

We would like to demonstrate the utility of this new paradigm approach by calculating results for two hypothetical cybersecurity investment intervention scenarios.

C. Return-On-Investment (ROI) Scenarios

Scenario One *(broad & shallow)* is a small ratings impact but broad intervention across a large number of hospitals based on three low-weighted vectors in the cybersecurity ratings algorithm which are approximately binary: SPF protocol implementation (1%), Desktop Software (3%), and Mobile Software (1%). Correctly configuring the SPF protocol to prevent email spoofing and having supported software on enterprise desktops/mobile devices are both

binary observations. A strategic intervention to satisfy these three vectors simultaneously (all three vectors originally unsatisfied) may result in an estimated modest cybersecurity ratings score increase of 20 points. This is a low intensity effort in resources at each hospital but treating more hospitals. Depending on the low-level treatment required at each hospital, it may be possible to accomplish treatment remotely via conferencing and shipment of equipment as needed.

Scenario Two *(focused & deep)* is a large ratings impact but focused intervention involving a small number of hospitals performing poorly in cybersecurity management. Prioritizing hospitals starting with the lowest cybersecurity rating and working upward intervening to bring each treated hospital up to the highest system rating prior to intervention. This is an intensive effort in resources at each hospital but treating less hospitals and less travel. Since this is a high level of treatment at each hospital, it cannot be accomplished remotely and will demand more time at each hospital.

TABLE II. SCENARIOS ONE/TWO STRATEGIC INTERVENTION RESULTS.

	IHS	**VHA**	**INTERSTATE**	**STATE**
SCENARIO ONE	YES-31	NO–21	NO-41	NO-85
SCENARIO TWO	YES-7	YES-9	YES-12	YES-18

Table II shows results from the two scenarios. The Scenario One intervention (a broad and shallow intervention consisting of a small treatment across a large number of hospitals) results in only one hospital system (IHS) increasing its mean ratings with statistical significance (after interventions at 31 hospitals). The Scenario Two intervention (a focused and deep intervention treatment consisting of a large treatment across a small number of hospitals) results in all four hospital systems increasing their mean ratings with statistical significance.

For these two scenarios, and an infinite number of other scenarios, ROI can be measured in cybersecurity ratings changes. Intervention investments can then be optimized, under a budget constraint, for evidence-driven strategic ROI cybersecurity management decisions.

V. CONCLUSION AND FUTURE WORK

In summary, we have introduced the use of cybersecurity ratings, based on cybersecurity metrics, to assess enterprise cybersecurity posture. Experimental results were demonstrated on large national infrastructures (U.S. hospital systems) where we empirically compared cybersecurity rating baselines for different large U.S. hospital systems. Lastly, we showed how interventions with cybersecurity investments can be strategically designed to improve cybersecurity and quantitatively measured for their ROI.

In the introduction, we raised challenges about the use of cybersecurity ratings which we address now. Cybersecurity ratings are a process, an algorithm with weighted cybersecurity metrics, thus if different metrics are proven to be more effective, then these new metrics can be easily substituted within the same process. Any qualitative or subjective cybersecurity aspect found to be important that may not be directly quantified, can be made measurable with analysis. We have shown multiple examples where cybersecurity ratings are meaningfully providing valuable baseline information for comparison and for calculating ROI. Unlike reputational rating systems, cybersecurity ratings are direct empirical measurements which cannot be gamed by adversaries without an adversary either having a successful man-in-the-middle spoofing capability or covert compromised control of the enterprise system being assessed to be able to manipulate metrics being measured.

For transparency, future work will provide more details on these algorithmic calculations including sensitivity of ratings to different weighting schemes and/or metric selections. We are also exploring dataset sharing options.

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] R. Anderson and T. Moore, "The Economics of Information Security," Science, Nov 2006.<doi: 10.1126/science.1130992>

[2] M. Blaze, "Afterword" within "Applied Cryptography 2nd Edition." by Bruce Schneier, 1996.

[3] INFOSEC Research Council, "Hard Problem List," Nov 2005.

[4] N. Mansourzadeh and A. Somayaji, "Towards Foundational Security Metrics," ACM New Security Paradigms Workshop, 2024.

[5] 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.

[6] N. Bartol, B. Bates, K. M. Goertzel, and T. Winograd, "Measuring Cybersecurity and Information Assurance," DoD Information Assurance SOAR Technology Analysis Center (IATAC), May 8, 2009.

[7] S. M. Bellovin, "On the Brittleness of Software and the Infeasibility of Security Metrics," IEEE Security & Privacy, 4(4) July/August 2006.

[8] D. J. Bodeau, R. D. Graubart, R. M. McQuaid, and J. Woodill, "Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring," MITRE Technical Report. Release Case No 18-2579, 2018.

[9] D. Chapin and S. Akridge, "How Can Security Be Measured?" Information Systems Control Journal, vol. 2 2005.

[10] J-H. Cho, P. Hurley, and S. Xu, "Metrics and Measurements of Trustworthy Systems," IEEE Mil Comm Conf (MILCOM), 2016.

[11] L. F. DeKoven et al., "Measuring Security Practices," Comm of the ACM, 65(9), 93-102, Sept 2022. <doi:10.1145/3547133>

[12] D. Flater, "Bad Security Metrics – Part 1: Problems," IEEE IT Professional, Jan/Feb 2018.

[13] D. Flater, "Bad Security Metrics – Part 2: Solutions," IEEE IT Professional, March/April 2018.

[14] F. Innerhofer–Oberperfler and R. Breu, "Potential Rating Indicators for Cyberinsurance: An Exploratory Qualitative Study," Workshop on the Economics of Information Security (WEIS), 2009.

[15] W. Jansen, "Directions in Security Metrics Research," NIST Internal Report 7564, April 2009.

[16] G. Jelen, "SSE-CMM Security Metrics," NIST and CSSPAB Workshop, Washington DC. 2000.

[17] R. Khudhair and A. Ahmed, "Overview of Security Metrics," Software Engineering, 4(4): 2016. <doi:10.11648/j.se.20160404.11>

[18] P. Manadhata and J. M. Wing, "An Attack Surface Metric," CMUCS-05-155, Carnegie Mellon University, 2005.

[19] M. Pendleton, R. Garcia-Lebron, J-H. Cho, and S. Xu, "A Survey on Systems Security Metrics," ACM Computing Surveys, 49(4), Dec 2016.

[20] S. L. Pfleeger, "Useful Cybersecurity Metrics," IEEE IT Professional, May/June 2009.

[21] S. L. Pfleeger and R. K. Cunningham, "Why Measuring Security is Hard," IEEE Security & Privacy, July/Aug 2010.

[22] A. S. Pope, R. Morning, D. R. Tauritz, and A. D. Kent, "Automated Design of Network Security Metrics," ACM Genetic and Evolutionary Computation Conference (GECCO), 2018.

[23] W. H. Sanders, "Quantitative Security Metrics: Unattainable Holy Grail or a Vital Breakthrough within Our Reach?" IEEE Security & Privacy, 12(2), March/April 2014. <doi:10.1109/MSP.2014.31>

[24] R. M. Savola, "Towards a Taxonomy for Information Security Metrics," Intl Conf on Software Engineering Advances (ICSEA), 2007.

[25] S. Schechter, "Quantitatively Differentiating System Security," Workshop on the Economics of Information Security (WEIS), 2002.

[26] D. Snyder et al., "Measuring Cybersecurity and Cyber Resiliency," RAND Corporation 2020. <doi:10.7249/RR2703>

[27] S. Stolfo, S. M. Bellovin, and D. Evans, "Measuring Security," IEEE Security & Privacy, 9(3) May/June 2011. <doi:10.1109/MSP.2011.56>

[28] M. Torgerson, "Security Metrics," 12th Intl Command and Control Research and Technology Symposium, 2007.

[29] R. B. Vaughn, A. Siraj, and D. A. Dampier, "Information Security System Rating and Ranking," CrossTalk: J of Defense Software Engineering, May 2002.

[30] R. B. Vaughn, A. Siraj, and R. Henning, "Information Assurance Measures and Metrics—State of Practice and Proposed Taxonomy," 36th Hawaii Intl Conf on System Sciences (HICSS-36), Jan 2003.

[31] G. O. M. Yee., "Designing Good Security Metrics," IEEE Annual Intl. Computer Software and Applications Conference (COMPSAC), 2019.

[32] J. Zalewski, S. Drager. W. McKeever, and A .J. Kornecki, "Measuring Security: A Challenge for the Generation," Fed Conf on Computer Science and Information Systems, 2014. <doi:10.15439/2014F490>

[33] National Institute of Standards and Technology (NIST), "National Vulnerability Database (NVD)/Known Exploited Vulnerabilities," Retrieved 3/24/24 from <https://nvd.nist.gov/general/news/cisa-exploit-catalog>

[34] MITRE, "CVE Program Mission," retrieved 3/29/24 from <https://www.cve.org/>

[35] National Institute of Standards and Technology (NIST), "Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology," NIST SP 800-40 Rev. 4, April 2022.

[36] M. S. Ragheb, W. Elmedany, and M. S. Sharif, "The Effectiveness of DKIM and SPF in Strengthening Email Security," 10th International Conference on Future Internet of Things and Cloud (FiCloud), 2023.

[37] S. J. Choi and M. E. Johnson, "The Relationship Between Cybersecurity Ratings and the Risk of Hospital Data Breaches," J of the American Med Informatics Assoc., 28(10), 2021.

[38] T. Hwang, S. J. Choi, and J. Lee, "The Impact of Data Breach on IT Investment at Neighboring Hospitals: Evidence from California Hospitals," Digital Health, 2025. <doi: 10.1177/20552076251375930>