RESOURCES FOR MEASURING CYBERSECURITY

A PARTIAL ANNOTATED BIBLIOGRAPHY

Kathryn Waldron

October 2019

R Street

TABLE OF CONTENTS

TABLE OF CONTENTS

OVERVIEW

Imagine the following scene: The Board meeting of any mid-sized American corporation. After discussing the important financial prospects for the coming quarter, the challenge of raw material supply and other matters on the agenda, the discussion turns to the company's cybersecurity posture. The following exchange takes place:

Board Member: *So, last year you budgeted $5 million to increase our cybersecurity. I see that this year you want another $7 million. Why?*

CEO: *Despite the expenditure last year, our Chief Information Security Officer says that there are still gaps in our security system that need fixing.*

Board Member: *That sounds reasonable, but tell me a bit more about last year. We spent $5 million. What did we get for it?*

CEO: *I'll let the CISO answer that.*

CISO: *We used that money to deploy a new intrusion detection system and upgrade our incident response protocols.*

Board Member: *And did it work? Are we actually safer now?*

CISO: *Yes we are.*

Board Member: *How do you know? How much improvement has there been? Can you quantify it?*

CISO: [silence] *Uh…let me get back to you on that.*

Obviously, this exchange is fictionalized, and our depiction of it is therefore blunter than is likely to occur in most Board rooms. But, the reality is not far off from this hypothetical exchange. Today, cybersecurity remains an art, rather than a science. We can qualitatively assess improvement, but the truth is that even moderately precise measures of cybersecurity remain elusive in that there is no generally agreed upon system of measurement that is—even metaphorically—equivalent to the concept of generally accepted accounting principles. Accordingly, if cybersecurity is to mature into a field where resource allocation and risk assessment are well-defined, a system of metrics will be required, which is to say we need a system that is:

- Objective;
- Capable of being quantified;
- Commensurate and intercomparable across different cybersecurity approaches and systems;
- Usable for decision-makers in allocating limited resources; and
- Widely agreed upon and generally accepted within the relevant communities.

As no such system currently exists, the R Street Institute has begun an initiative intended to build a consensus around how to fill that gap.

As with any such effort, our multi-pronged approach to this critical issue begins…at the beginning. Therefore, in this partial bibliography, we attempt to compile a baseline of existing disparate measurement efforts. In so doing, we have sought to both summarize the existing field and characterize it. At the outset, it is important to emphasize that our intent here is neither comprehensive nor overtly technical in nature. We do not purport to have fully defined the field, nor have we tried to plumb the depths of technical intricacy. Rather, our goal is to provide a systematic overview of the field that is both technically literate and of use to decision-makers in the public and private sectors.

We began by asking: How are firms currently measuring their cybersecurity? In general, they continue to use qualitative measures of security rather than quantitative ones. For example, in one 2015 survey of Chief Intelligence Systems Officers (CISOs) (concededly a slightly dated inquiry), industry best practices and frameworks were ranked as the primary drivers that determined their organization's cyber needs. [1]

Quantitative methods (including both quantifications of Return on Investment [ROI] and more complex methods) of measuring security controls were ranked only fourth on the list, and many of those interviewed expressed skepticism about the usefulness and accuracy of quantitative methods. One CISO in particular suggested that quantitative methods were not effective in galvanizing management or board members. Here at R Street Institute, however, we are of the tentative view that this perspective is shortsighted. Without accurate, standardized methods to measure cybersecurity, detecting and deterring cyber threats will continue to be more art than science.

Although the breadth of academic and professional interest prompted by this increasingly salient issue prevents this bibliography from being all encompassing, the partial attempt will shed light on some of the most pervasive and exciting work that has been and is currently being done.

[1] Tyler Moore et al., "Identifying How Firms Manage Cybersecurity Investment," Oct. 28, 2015, p. 10.

GENERAL METHODOLOGY

We break our review into several sections that reflect different approaches that have been adopted and characterize the literature in the following three ways:

First, there is a strong divide between methods that apply ex ante and those that apply ex post. In other words, some measurement methodologies look prospectively at security measures to assess how changes in security will impact an enterprise. Others look retrospectively at security after a measure has been implemented and then try either to measure the positive increase or, in some cases, the injury that has occurred and its valuation. The reasoning of the latter, of course, is that if a new security implementation reduces the injury experience, a proxy measure of how to value the new tool has been created.

Second, some measures assess security exclusively as a process value—creating frameworks and checklists of factors that are thought to improve security and measuring compliance rates with these second-order indicia of security. By contrast, a far smaller number of efforts try to look at security directly, asking whether or not a new addition to the security of an enterprise affirmatively increases the ability to stop intrusions or the like.

Third, and finally, buried within some of these efforts is a different, more fundamental distinction. For while some of these measures focus exclusively on indicia of prevention, a few look instead at resiliency. In other words, at least one strand of cybersecurity metric quantification looks not at how much was stopped but rather at how quickly the system was restored. If the fundamental of metrics is that an enterprise maximizes what it measures for success, one critical question, then, is to define success properly. Thus, at some level, we will need to consider whether prevention or resiliency is a superior security value.

Using this construct, we have identified and categorized several different methods currently in use to quantify cybersecurity. Roughly speaking they fall into the following groups:

1. **Frameworks and Scorecards**—These methods are mostly focused on measuring compliance with some baseline set of best practices. Some operate prospectively, others retrospectively. Almost none directly measure security.
2. **Insurance Metrics**—These methods are a relatively unique subset of many others, used as models within the insurance industry to quantify risk and set insurance premiums. As such, they incorporate aspects of other systems of measurement and vary widely.
3. **ROI/ROSI**—These methods rely on traditional business models to measure a return on investment for an enterprise. Since security improvements are hard to quantify, some ROI systems have been modified to measure a "return on security investment." Almost all of these models are prospective and predictive in nature..
4. **Cyber Crime**—One alternate method of measuring risk reduction is to attempt to measure it directly by an ex ante compilation of harms and, over time, reductions in that metric. Most efforts of this sort involving cybersecurity have been derived from metrics about the loss from cyber crime.
5. **CYRIE**—We reserve a special section for a series of academic and practical studies that are being conducted by the Department of Homeland Security (DHS). The Cyber Risk Economics project supports research into the economics of cyber threats and information security, with a particular focus on measurement and evaluation of the impact of security investment on risk probabilities and the effectiveness of security controls.
6. **Others**—Finally, we include a catch-all section of measurement systems that do not fall into any easily defined category.

FRAMEWORKS & SCORE CARDS

Because it is difficult to accurately assess cyber risk in easily understood quantitative terms, many companies are calling for or relying on industry standards. Put simply, these kinds of frameworks give companies a standard against which to compare. And, this push has given rise to the use of scorecards to measure a company's information security practices. Companies can create their own scorecards based on the National Institute for Standards and Technology (NIST)cybersecurity framework [2] or outsource scorecard evaluation to one of several companies.

While useful as an evaluation tool, frameworks and scorecards are ripe for misuse. (This is not surprising, given Campbell's law: "the more any quantitative social indicator is used for social decision-making, the more subject it will be to corruption pressures and the more apt it will be to distort and corrupt the social processes it is intended to monitor.") [3] By their very nature, frameworks are broad-sweeping and may not aid firms' selection of particular security investments. Empirical studies of the effectiveness of frameworks and scorecards is limited because widespread adoption is still a recent phenomenon. Incorrectly applied, frameworks can grant companies a false sense of security, as managers believe themselves to be more secure than they really are. This phenomenon can be seen in government, as detailed in a GAO report on cyber vulnerabilities in DOD weapon systems. [4] (This need to comply with a set of predetermined standards could also actually harm a company's security and performance if they install new security programs without uninstalling old ones.) [5]

On the other hand, frameworks and scorecards can serve as a good indicator of vulnerability to managers and business owners who are concerned with a lack of cyber security controls. Particularly for small and mid-sized enterprises, a scorecard or toolkit can be an easy way of rapidly improving cybersecurity by identifying areas where simple changes are likely to enhance security even if not in readily measurable ways.

Finally, frameworks may encourage an enterprise to overinvest in cybersecurity—there may well be some cyber risks so unlikely to occur or that would result in such small amounts of loss that it would not be cost effective for a company to protect against them. Therefore, frameworks aimed at wholly eliminating cyber risks may not accurately guide companies as to how to spend a security budget effectively.

Below we have included a list of some of the most common frameworks and scorecards. Note that this list is not exhaustive, as new ones are being developed all the time. Furthermore, inclusion on this list in no way equals a recommendation on behalf of R Street Institute.

[2] Jeff Wagner, "Developing a Cybersecurity Scorecard," U.S. Dept. of Agriculture, Aug. 17, 2017, p. 3.
[3] Donald T. Campbell, "Assessing the impact of planned social change," *Evaluation and Program Planning 2:1* (1979), pp. 67-90.
[4] "Weapon Systems Cybersecurity DOD: Just Beginning to Grapple with Scale of Vulnerabilities," U.S. Govt. Accountability Office, Oct. 10, 2018.
[5] Serge Malenkovich, "Why Using Multiple Antivirus Programs is a Bad Idea," Kaspersky Lab Daily, Sept. 9, 2013.

NIST

Matthew P. Barrett, *Framework for Improving Critical Infrastructure Cybersecurity* 1.1, National Institute of Standards and Technology, April 16, 2018, pp. i-48.

Created in 2014 in response to Executive Order 13636, the National Institute of Standards and Technology (NIST) framework is one of the most well-known and widely adopted frameworks. It breaks down the process of accessing a company's cyber capacities and needs into five core steps (identify, protect, detect, respond and recover) but recognizes that each company will need to apply the framework in different ways to best service their own unique needs.

FAIR Institute

Jack Freund and Jack Jones, *Measuring and Managing Information Risk: a FAIR approach* (Butterworth-Heinemann, 2014)

The Factor Analysis of Information Risk (FAIR) model differs from other frameworks because it is an analytical risk model rather than a Capability Maturity Model (CMM) or checklist of controls. Accordingly, instead of providing an organization with an ordinal ranking or list of best practices, the FAIR model is designed to provide "financially derived results." Available FAIR tools include the above-referenced book and an online training program known as *FAIR-U*.

Cobit

"Introducing Cobit 2019," Information Systems and Control Association, 2019.

The Control Objectives for Information and Related Technologies (COBIT) were developed by the Information Systems and Control Association (ISACA) in 1996. COBIT 5 was released in 2012; the most recent update, COBIT 2019, came out in December 2018 and was updated to include new technologies and systems, to better match current global standards and to incorporate an "open-source" model to allow for continual feedback and updates.

International Organization for Standardization

"ISO/IEC 27000 family - Information security management systems," International Organization for Standardization, 2018.

The ISO/IEC 270000 family of standards were developed jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) to help organizations protect sensitive information by managing the risks posed by people, processes and IT systems. Organizations can also choose to be audited and certified against these standards to prove compliance.

Center for Information Security

"Cybersecurity Tools," Center for Information Security, 2019.

The Center for Information Security offers both their CIS Controls and CIS Benchmarks as tools to measure a firm's security. The CIS Controls is a list of twenty controls organizations can employ to better protect against cyberattacks. The CIS benchmarks provide more comprehensive frameworks tailored to a targeted system. These benchmarks are developed through the volunteer efforts of various information security specialists.

Global Cyber Alliance

"GCA Cybersecurity Toolkit for Small Business," Global Cyber Alliance, 2019.

GCA's toolkit is targeted at small and mid-sized enterprises and is intended to use Center for Internet Security Controls (CIS Controls, see above) to enable business owners to reduce common cyber risks. The CIS Controls are a recommended set of actions, built and continuously updated using current threat information and expert guidance, to prevent and/or reduce the most common attacks in today's cyber threat landscape.

TC CYBER

"Cyber security," European Telecommunications Standards Institute, 2019.

The ETSI Cyber Security Technical Committee (known as TC CYBER) was created in 2014 to focus on providing international standards, particularly in Europe. Their standards cover the security of a range of infrastructure, devices and services; they also have a subgroup that focuses specifically on the risks posed to cryptography by quantum computing.

ISF Standard of Good Practice for Information Security

"The ISF Standard of Good Practice for Information Security 2018," Information Security Forum, 2018.

Since the 1990s, the Information Security Forum (ISF) has been publishing a list of information security best practices, which they update every two years. The 2018 edition discusses the standards set out by the ISO/IEC 27002:2013, NIST Cybersecurity Framework, CIS Top 20, PCI DSS and COBIT 5.

SWIFT Customer Security Control Framework

"SWIFT publishes cybersecurity counterparty risk guide," SWIFT, 2019.

SWIFT's Customer Security Control Framework (CSCF) "establishes a security baseline of mandatory and advisory controls for the entire user community, against which SWIFT users are required to self-attest their compliance on an annual basis." SWIFT recently released a guide to "Assessing Cybersecurity Counterparty Risk" based upon their framework. (Assessing counterparty risk is an especially important issue given that many companies may use different standards and controls for their cybersecurity. Counterparty risk thus increases as the number of external partnerships increases.)

The Software Alliance

"BSA Framework for Secure Software," BSA, 2019.

BSA's software framework is an effort to evaluate software security across the entire software lifecycle. It is particularly innovative in that it attempts to define a desirable end state for software lifecycle security issues in a way that is capable of express measurement.

American Public Power Association

"Cybersecurity Scorecard," American Public Power Association, 2019.

Based off the Dept. of Energy's *Electricity Subsector Cybersecurity Capability Maturity Model* (ES-C2M2), this is an online self-assessment tool designed for public power utilities to "assess cyber risk, plan improvements, prioritize investments, and benchmark their security posture."

BitSight

"BitSight Security Ratings," BitSight, 2019.

BitSight rates each company on a scale from 250 to 900, using externally observable data to look for evidence of compromised systems and data breaches. It also provides "diligence details," wherein BitSight analyzes a firm's security configurations (such as SSL, SPF, DKIM, DNSSEC etc.) to measure effectiveness.

FICO

"FICO® Cyber Risk Score," FICO, 2019.

FICO's Cyber Risk Score builds a risk profile based off of data collected from the internet that looks at key risk indicators such as the health and hygiene of IT systems, network infrastructure, and software and services. This risk profile is then compared against historic data to forecast the likelihood of future breaches. FICO is currently offering to provide organizations with a Cyber Risk Score free of charge.

F-Secure

"THE CYBER SECURITY Stress Test," F-Secure, 2019.

This is a 20-question survey designed to help IT professionals locate gaps in their security strategies. Each organization's answers are compared against industry statistics and then the organization is rated on a scale from 1 to 5, assessing that organization's ability to predict, prevent, detect and respond to cyberattacks.

NormShield

"Home Page," NormShield, 2019.

Normshield offers two cyber scorecards, both of which rate companies from A to F in a variety of categories. The Rapid Cyber Risk scorecard evaluates a company in 60 seconds, covering 11 categories and considering over 250 security checklist items. The Comprehensive Cyber Risk scorecard, which takes a few minutes to complete, covers 20 categories and over 500 security checklist items.

RiskLens

"Risk Portfolio," RiskLens, 2019.

RiskLens is the only cyber risk management software built upon the FAIR model. The platform has four components: model the organization's risk environment, develop potential risk scenarios, run simulations and generate risk analytics reports. To do this, the program incorporates "maturity models, template-based best practice workflows, advanced quantitative risk analytics, industry-specific loss data [and] data integration capabilities."

BitSight

"BitSight Security Ratings," BitSight, 2019.

SecurityScorecard is a "report card" of a firm's security risk profile, based off publicly available and proprietary security risk intelligence sources. Firms are given a letter grade from A to F for the following ten different security categories: network security, DNS health, patching cadence, endpoint security, IP reputation, web application security, cubit score, hacker chatter, leaked credentials and social engineering.

UpGuard

"BreachSight," UpGuard, 2019. "VendorRisk," UpGuard, 2019.

UpGuard's BreachSight scans over 50 sources for leaks or breaches. A dedicated security expert then assists each organization to assess results and correct security gaps. UpGuard's products also include VendorRisk, a program that offers the opportunity to survey and track the scores of an organization's vendors and to be notified immediately if their scores drop.

CYBER INSURANCE METRICS

Cyber insurance is a blossoming field—in 2017, for example, the number of direct premiums written in the U.S. cybersecurity market rose nearly 32 percent from the previous year.[6] A 2018 FICO study found that 76 percent of all surveyed U.S. executives said their company had cyber insurance, an increase from only 50 percent in 2017. However, the increase in cyber coverage was not uniform across industries. Seventy percent of healthcare companies revealed they lacked any type of cyber insurance.[7] Given the growth in this field, it should come as no surprise that much of the research focused on quantitative assessments of cyber risk come from this sector of business and academia.

However, the mere existence of the cyber insurance industry does not mean that standardized quantitative methods, compared to other insurance industries, are being used. As one article reports: "Cybersecurity insurance has no standard scoring systems or actuarial tables."[8] This is partially because cyberattacks have only been a serious risk for companies for a relatively short time, and partially because companies may be reluctant to share data when they are attacked, as they are afraid of additional repercussions, such as loss of market share or reputation.

[6] "U.S. Cyber Market Grew 32% in 2017 But Most Small-Medium Firms Opted Out: A.M. Best," *Insurance Journal*, May 21, 2018.
[7] "FICO Survey: Most US Firms Have Cybersecurity Insurance—But Only 1 in 3 Say It Is Full Coverage," FICO, Aug. 21, 2018.
[8] Maochao Xu and Lei Hua, "Cybersecurity Insurance: Modeling and Pricing," Society of Actuaries, April 2017, pp. 4-5.

"Cyber Insurance: Recent Advances, Good Practices & Challenges," European Union Agency for Network and Information Security, November 2016.

This ENISA report discusses best practices proposed by European cyber insurance companies.

Rainer Böhme and Galina Schwartz, "Modeling Cyber-Insurance: Towards A Unifying Framework," *Harvard University Workshop on the Economics of Information Security*, June 7, 2010.

This framework was developed to classify market models of cyber insurance, looking specifically at a model's interdependent security, correlated risk and information asymmetries. The authors find that existing cyber-insurance markets tend to adversely impact incentives for firms to improve their own security.

Angelica Marotta et. al., "Cyber-insurance survey," *Computer Science Review 24* (May 2017), pp. 35-61.

Marotta et al. provide a brief history of the cyber insurance industry and a survey of existing academic literature on the subject. They also discuss the unique challenges of cyber insurance compared to other types of insurance.

Ranjan Pal et al., "Will Cyber-Insurance Improve Network Security? A Market Analysis," *IEEE International Conference on Computer Communications,* April 29, 2014.

Pal et al. are skeptical that the existence of a cyber insurance market will lead to a greater amount of cybersecurity. They predict competitive markets lack an efficient equilibrium, while insurers in monopoly markets will make zero profits, disincentivizing them from entering the market at all.

ROI/ROSI

A quick look at articles and websites reveals that there is disagreement about how to calculate risks related to cybersecurity, and even whether it is possible to calculate it at all. Accordingly, businesses looking for formulas to assist with measuring cybersecurity will often first run into variations on standard ROI (return on investment) formulas. And, in fact, Christopher Porter, Vice President and CISO at Fannie Mae, advocated this method at an MIT symposium last year, where he projected a savings of approximately $20 million annually through their cybersecurity system.[9]

However, the simplicity of ROI's terminology is simultaneously appealing and confusing when it comes to cybersecurity. Calculating "benefits" may seem impossible or inappropriate since companies cannot measure profits from investing in cybersecurity—only the avoidance of loss. The original goal of ROI is not adequate for business owners or IT professionals who are generally making decisions with the singular goal of minimizing risk. This has led to the development of the return on security investment (ROSI), a variant of the ROI formula specific to security issues.

ROSI calculates a quantitative risk assessment and then looks at the cost of investing in a specific security measure to protect against the risk. The company's annual loss expectancy (ALE) is then calculated, which is equal to the amount of money a company will lose in each attack multiplied by the number of attacks predicted each year. The mitigation ratio is the percentage of attacks blocked by the security investment in question. Multiplied together, they represent the expected loss a company might face without the particular security control. But security controls are not free—hence the need for subtracting and then dividing by the cost of the security control, which puts the prevented loss in the context of a business's budget.

While the ROI/ROSI method can help business owners and board members easily understand the costs of not having cybersecurity, these methods are not problem free. They depend upon an accurate estimate of both expected loss (whether a direct loss or a reputational harm), and the number and types of attacks a company will face. If calculated with past data, they may not adequately predict optimal use of security resources in the future. Further, as security experts patch and protect previous vulnerabilities, hackers evolve their methods, seeking new vulnerabilities to exploit. New technologies, including the ever-more-connected Internet of Things, can also change the threat landscape. Because of this, using data from last year's information security success may not be enough to ensure next year's.

[9] Christopher Porter, "Measuring ROI for Cybersecurity: Is It Real or a Mirage?" *MIT Sloan CIO Symposium*, May 24, 2017.
[10] Science and Technology Directorate, "Cyber Risk Economics Capability Gaps Research Strategy," U.S. Dept. of Homeland Security, 2018, pp. 1-44.

In some cases, obtaining accurate data may be nearly impossible. A company's cyber risk is highly dependent upon the vulnerability of its greater network, including third-party contractors. A malware attack on a contractor's software may leave a company bearing some of the cost of a denial-of-service attack, but this possibility is hard to incorporate in ROI/ROSI formulas since knowledge about outside firms' cyber risks may be difficult to obtain or estimate: "Estimates of risk or harm all too often mistakenly induce systemic risk by amassing specific risks or use attributes that do not map to real risk (e.g., using a company's market share rather than company-specific risk attributes to assess aggregate risk)."[10] Industry reports may provide some guidance for estimation, but are likely to underreport the actual number of attacks an industry faces as firms may be reluctant to share the extent of breaches. (And some firms may not be aware of cyber breaches at all).

Nonetheless, while the ROI/ROSI methods may not be as accurate at assessing the costs and benefits of a particular cyber solution, the method's simplicity has great appeal.

ROI/ROSI RESOURCES

"Introduction to Return on Security Investment," European Union Agency for Network and Information Security, Dec. 12, 2012, pp. 1-14.

This report walks readers through both return on investment (ROI) and return on security investment (ROSI) formulas. Brief attention is given to the limitations of the model. Critiques of the Gordon and Loeb model (annotated below) are used as justification for the superiority of ROSI.

Pascal Brangetto and Mari Kert-Saint Aubyn, "Economic Aspects of National Cyber Security Strategies," NATO Cooperative Cyber Defence Centre of Excellence, October 2015, pp. 9-16.

This report contains a discussion of the ROI/ROSI model, as well as a handful of other metrics governments may want to use to develop national strategies.

Wes Sonnenreich et al., "Return on security investment (ROSI)-a practical quantitative model," *Journal of Research and practice in Information Technology* 38:1 (February 2006), pp. 45-56.

This paper includes several examples of how firms can quantify lost productivity when calculating ROI/ROSI.

ANALYZING THE COST OF CYBERCRIME

Another generic attempt to measure cybersecurity is through the measurement of forecasted loss and through further efforts to measure how well (or poorly) new security systems tend to mitigate that loss. Thus, we see many efforts to measure the financial losses incurred by enterprises—whether through direct monetary loss or through losses in intellectual property. Generally, these efforts are only partially successful, at least in part because criminal losses are often not systematically reported.

CYBER LOSS RESOURCES

Ross Anderson et al., "Measuring the Cost of Cybercrime," *Berlin Brandenburg Academy of Sciences Workshop on the Economics of Information Security*, June 26, 2012.

Anderson et al. present a systematic study of the costs of cybercrime, wherein they find that "traditional crimes" like tax and welfare fraud tend to cost citizens more than prevention, while defending against "transitional" and "new" cybercrimes, such as payment card fraud or fake antivirus software, is often more expensive than the damage resulting from the actual crimes.

Claudia Biancotti, "The price of cyber (in)security: *evidence from the Italian private sector,*" Bank of Italy Occasional Papers, Nov. 29, 2017, pp. 1-43.

This case study of cyber risk in the Italian private, non-financial sector looks at median expenditure on cyber defense, and finds a wide variation of spending based off firm size, industry sector, awareness of cyber threat and history of attacks.

Paul Dreyer et al., "Estimating the Global Cost of Cyber Risk: Methodology and Examples," RAND Corporation, 2018, pp. i-54.

Using data from the Organization for Economic Co-operation and Development, this report estimates the current and future global costs of cyber risk by looking at both the country and industry sectors. Costs are measured as a part of a country's Gross Domestic Product (GDP), with the global cost of cybercrime amounting to GDP costs of $275 billion to $6.6 trillion and total GDP costs (direct plus systemic) of $799 billion to $22.5 trillion (1.1 to 32.4 percent of GDP).

Eric Jardine, "Mind the denominator: towards a more effective measurement system for cybersecurity," *Journal of Cyber Policy* 3:1 (May 8, 2018), pp. 116-39.

Jardine argues that cybercrime metrics, such as the number of phishing websites, are often misleading as they are not appropriately normalized for the population of the city or country being studied. This failure to normalize statistics distorts our sense of the cyber "ecosystem," exacerbating our sense of how frequently cybercrime occurs.

Kenneth D. Nguyen et al., "Valuing information security from a phishing attack," *Journal of Cybersecurity* 3:3 (Nov. 1, 2017), pp. 159-71.

This study surveyed internet users for the "security premium" or maximum price they were willing to pay to protect information from phishing attacks. The authors also ran an experiment on Amazon Mechanical Turk users, asking them to make choices between conflicting trade-offs (security vs. cost, for example) to assess a willingness to pay for security.

Marcus Riek et al., "Estimating the costs of consumer-facing cybercrime: A tailored instrument and representative data for six EU countries," *University of California, Berkeley Workshop on the Economics of Information Security*, June 12, 2016, pp. 1-43.

The authors analyze types of cybercrime in six European countries to measure the cost of consumer-facing cybercrime, finding that the majority results in losses of time rather than money. Furthermore, they find the cost of preventive protection generally exceeds the losses felt by cyber victims.

CYRIE

Launched in 2017, CYRIE is the Cyber Risk Economics project run by the Department of Homeland Security Science and Technology Directorate. The project supports research into the economics of cyber threats and information security, with a particular focus on measurement and evaluation of the impact of security investment on risk probabilities, and the effectiveness of security controls. CYRIE funds projects at the University of Tulsa, University of Michigan and 418 Intelligence, among other partners.

CYRIE RESOURCES

Science and Technology Directorate, "Cyber Risk Economics," Dept. of Homeland Security, 2019.

Erin Kenneally et al., "Cyber Risk Economics Capability Gaps Research Strategy," *IEEE: International Conference On Cyber Situational Awareness, 2018*, pp. 1-6.

PROJECT DESCRIPTIONS

University of Tulsa

"This effort is studying data usage and production by researchers to construct a better picture of the value of and prospects for cybersecurity data-sharing. The effort will examine the published research literature to identify what data is being produced to understand the data that can be shared, how we are falling short, and ultimately recommend how sharing can be improved to enhance evidence-based policy and technology solutions. Additionally, the effort will analyze usage of the research data stewarded by CSD's Information Marketplace for Policy and Analysis of Cyber-risk & Trust project to understand how existing datasets are being leveraged by others when shared. Last, the effort will empirically estimate the costs associated with data-sharing using information gathered by DHS."[11]

[11] Science and Technology Directorate, "Cyber Risk Economics," U.S. Dept. of Homeland Security, 2019.

NormShield

❝ Cyber insurance is a method for transferring and mitigating cybersecurity risks and a potential incentive mechanism for internalizing the externalities of security investments. This effort will tackle some of the most significant challenges to cyber insurance. The technical approach consists of developing risk-informed insurance policies that are derived from theoretically-sound, yet practical algorithms. It also addresses risk-aggregation via empirical and analytical studies aimed at extracting interdependencies and embedding this acquired understanding in the modeling of aggregated risk of a portfolio of insurance policies. The results are intended to make concrete progress toward a quantitative risk-assessment tool that is needed to effectively mitigate moral hazard for the insurance industry." [12]

418 Intelligence

❝ This effort will prototype and pilot a crowdsourced solution for the problems of understanding the real-world effectiveness and value of cybersecurity controls. It will develop a novel game-based forecasting prototype platform and user experience that will engage participants in competition and mastery of the latest developments in cybersecurity. This prototype will be backed up by anonymous information-sharing made safe by a data encryption technology designed to enforce complete control over the digital rights to information while in-motion and at-rest. The approach will engage stakeholders in an ongoing, risk-oriented experience where incentives [are] based in a game economy. It will result in real benefits that will drive exchanging high-value information on cybersecurity controls that currently are opaque and stove-piped." [13]

University of California

"University of California, San Diego was awarded $1,045,015 for a multi-year effort to develop threat intelligence tools and techniques for measuring the reliability and value of a threat intelligence source to an enterprise. The project will include four kinds of metrics—technical, comparative, operational and risk—to allow end-users to compare different threat intelligence products reliably; ultimately increasing transparency and incentivizing more effective controls within the threat intelligence market place."[14]

University of Illinois

❝ University of Illinois, Chicago was awarded $227,305 for a twelve-month effort to develop a cyberattack economic impact model, and a tool to automate data collection and analysis in order to provide near real-time estimates of cyberattack outcomes. The model and reference implementation will provide a standard baseline against which organizations can evaluate and quantify estimated economic impacts of cyberattacks for cybersecurity investment decision support."[15]

[12] Science and Technology Directorate, "Cyber Risk Economics," U.S. Dept. of Homeland Security, 2019.
[13] Ibid.
[14] Science and Technology Directorate, "News Release: DHS S&T Awards $1.27M to Two Universities to Improve Cybersecurity Investment Decision Making," U.S. Dept. of Homeland Security, Nov. 8, 2018.
[15] Ibid.

OTHER RESOURCES

ADDITIONAL MEASUREMENT EFFORTS

TruSTAR

"About TruSTAR," TruStar, 2019.

TruSTAR is an intelligence platform created to help security teams incorporate machine learning and automation into their system. To do so, it uses its "enclave knowledge management architecture" to share information traditionally siloed away to encourage better security collaboration. Enclaves "streamline collaboration and provide enrichment from clients' trusted data sources" while also operationalizing "threat intelligence data shared from external sources like commercial feeds, OSINT and ISAC/ISAO data."[16]

Listed below is a partial list of some of the other academics working to develop better quantitative methods.[17]

ACADEMIC WORK

Terrence August et al., "Market Segmentation and Software Security: Pricing Patching Rights," University of California, Berkeley / ICSI Workshop on the Economics of Information Security, June 14, 2016, pp. 1-40.

In this paper, the authors discuss the effectiveness of patching, noting that the customer's current choice whether or not to apply a patch lacks incentives to promote security. They also suggest how to appropriately price patching "rights" to reward individuals who relinquish the right to choose which patches to adapt in favor of automatic updates.

Matthias Brecht and Thomas Nowey, "A Closer Look at Information Security Costs," Berlin Brandenburg Academy of Sciences Workshop on the Economics of Information Security, June 26, 2012, pp. 1-21.

Acknowledging the lack of a common model of information security, Brecht and Nowey discuss four approaches for firms to assess information security costs. They propose two metrics and conclude with a list of suggestions for further research.

---

[16] Lianna Catino, "Cyber Defense Magazine Names TruSTAR the Next-Gen Threat Intelligence Leader of 2018," Press Release, Oct. 3, 2018.

[17] Many of the academic works listed in this section are papers or presentations given at Workshop on the Economics of Information Security (WEIS). With conferences held annually since 2002, WEIS is "the leading forum for interdisciplinary scholarship on information security and privacy, combining expertise from the fields of economics, social science, business, law, policy, and computer science." WEIS workshops allow scholars from a variety of backgrounds to present novel research and propose tools to deepen our understanding of the inherent trade-offs involved with information security, including cybersecurity. We have highlighted several pieces of research we view as particularly salient. In addition to the pieces listed below, topics addressed at past workshops include "the role of incentives between attackers and defenders of information systems, identified market failures surrounding Internet security, quantified risks of personal data disclosure and assessed investments in cyber-defense." See: "Call for papers," Workshop on the Economics of Information Security, 2019.

Melissa Carlton et al., "Development of the MyCyberSkills™ iPad app: A scenarios-based, hands-on measure of non-IT professionals' cybersecurity skills," *Pre-International Conference of Information Systems SIGSEC-Workshop on Information Security and Privacy*, December 2015, pp. 1-12.

Carlton et al. propose to create an iPad application, known as MyCyberSkills, which would measure an individual's cybersecurity skills through hands-on tasks related to key skills as identified by information security experts. After completing these tasks, developed from real-life scenarios, each person will be scored. The app is still in development.

Brian Chess, "Metrics That Matter: Quantifying Software Security Risk," *Proceedings of Workshop on Software Security Assurance Tools, Techniques, and Metrics*, February 2006, pp. 22-28.

Chess discusses the flaws of three current approaches for measuring software security: penetration testing, routine quality assurance testing and what he calls the "feel-good" metric. He then proposes a new set of metrics that utilize source code analysis.

Adéle Da Veiga, "A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument," ExCel London: SAI Computing Conference, July 15, 2016, pp. 1006-15.

Da Veiga develops a cybersecurity culture research methodology (CSeCRM) that will assess an organization's security culture. With the CSeCRM method, each organization develops questionnaires about their firm to assess employee understanding of security policies and best practices.

Melissa Hathaway et al., "CYBER READINESS INDEX 2.0," Potomac Institute for Policy Studies, November 2015.

This is an index that evaluates each country's cyber readiness. It is built on over seventy indicators, including a country's policies, laws, standards and regulation. Currently, the index has been used to assess the states of over 125 countries around the world.

Lukas Demetz and Daniel Bachlechner, "To Invest or Not to Invest? Assessing the Economic Viability of a Policy and Security Configuration Management Tool," Berlin Brandenburg Academy of Sciences Workshop on the Economics of Information Security, June 26, 2012, pp. 1-35.

The authors compare current approaches to evaluating information security investments. As their standard, they hold that an ideal approach would "allow that the investment is made as a whole, consider financial and non-financial measures, take one time and running costs and benefits into consideration, be applicable without considering attacks" and "take network effects of the investment into account." They find that none of the approaches matches these standards.

Summer Fowler and Peter P. Chen, "CsPI: A New Way to Evaluate Cybersecurity Investments: A Position Paper," *IEEE International Conference on Software Quality, Reliability and Security Companion*, July 26, 2017, pp. 283-84.

Fowler and Chen created the Cybersecurity Performance Index (CsPI) as a cybersecurity counterpart to a "Cost Performance Index" or "Schedule Performance Index" for earned value. Their new method proposes to evaluate cybersecurity expenses against a plan built around "protect, detect, respond and recover" goals.

Lawrence A. Gordon and Martin P. Loeb, "The Economics of Information Security Investment," *ACM Transactions on Information and System Security* 5:4 (November 2002), pp. 438-57.

Gordon and Loeb develop their own model to optimize the amount a firm should spend on information security. According to their model, firms can maximize economic returns by focusing security on mid-level risks rather than high-level ones. They also suggest firms should only spend "a small fraction of the expected loss due to a security breach."

Lawrence A. Gordon et al., "Externalities and the magnitude of cyber security underinvestment by private sector firms: a modification of the Gordon-Loeb model," Journal of Information Security 6:1 (2015), pp. 24-30.

Here, Gordon et al. defend the Gordon-Loeb model, arguing that when it is modified to account for externalities, an organization's "optimal investment in cyber security increases by no more than 37% of the expected externality loss."

Douglas W. Hubbard and Richard Seiersen, *How to Measure Anything in Cybersecurity Risk (John Wiley & Sons, 2016)*. Presentation Slides

Hubbard and Seiersen warn that incorrect risk metrics and measurements may lull organizations into a false sense of security. Accordingly, they propose to measure risk using a method based off Monte Carlo simulations.

Rolf Hulthén, "Communicating the Economic Value of Security Investments; Value at Security Risk," Dartmouth College Workshop on Economics of Information Security, June 26, 2008, pp. 1-12.

According to Hulthén, companies have underinvested in security in the past because the average manager struggles to understand the highly technical and specialized field of information security. This has led to a reliance on Return on Investment (ROI) as the security metric of choice, despite its significant flaws. Hulthén argues that managers have a superior metric on hand: Value-at-Risk.

Husin Jazri et al., "Measuring Cybersecurity Wellness Index of Critical Organisations," *IST-Africa Week Conference*, May 9-11, 2018.

The authors discuss the concept of "cybersecurity wellness." Using data from twenty companies, they create an index scorecard of cybersecurity vital signs, which they measure on a Likert scale, assigning each sign a value from 1-3.

Jan Willemson, "Extending the Gordon & Loeb Model for Information Security Investment," *The Fifth Workshop on the Economics of Information Security*, June 26, 2006, pp. 1-12.

In their model, Gordon and Loeb suggest that a universal limit may exist on the optimal amount organizations should spend on security. They also propose that limit might be 8 percent of expected loss. Willemson critiques this number by demonstrating scenarios where an organization might be better served by spending 50 percent of expected loss.

ABOUT R STREET

The R Street Institute is a nonprofit, nonpartisan, public-policy research organization ("think tank"). Our mission is to engage in policy research and outreach to promote free markets and limited, effective government. In addition to our D.C. headquarters, we have offices in Georgia, Texas, Ohio, Massachusetts and California, covering the Southeast, Central, Midwest, Northeast and Western regions, respectively.

We work extensively on both state and national policy, focusing on issues that other groups tend to neglect. Our specialty is tackling issues that are complex, but do not necessarily grab major headlines. These are the areas where we think we can have a real impact. We believe free markets work better than the alternatives. At the same time, we recognize the legislative process calls out for practical responses to current problems. Toward that end, our motto is "Free markets. Real solutions."

INDEPENDENCE STATEMENT

The R Street Institute is committed to producing high-quality research and educating federal, state and local policymakers. Facts, data and staff expertise drive our research. We do not and will not permit the interests of politicians, donors or any other third party to dictate R Street's research or policy positions. While R Street may solicit input from any number of interested stakeholders, we are solely responsible for our research and related activities. Even where we agree with stakeholders and donors, R Street staff does not and will not represent, lobby or advocate on behalf of any third party.

Kathryn Waldron is a fellow at the R Street Institute, where she researches and writes on cybersecurity, space and other national security policy issues.

R STREET INSTITUTE
1212 New York Avenue, NW, Suite 900
Washington, D.C. 20005
(202) 525-5717 feedback@rstreet.org
www.rstreet.org