Return on Cybersecurity Investment in Operational Technology Systems: Quantifying the Value That Cybersecurity Technologies Provide after Integration

Roger A. Hallman[1,2], Maxine Major[2], Jose Romero-Mariona[2], Richard Phipps[2], Esperanza Romero[2] and John M. San Miguel[2]

[1]*Thayer School of Engineering, Dartmouth College, Hanover, New Hampshire, U.S.A.*

[2]*Naval Information Warfare Center Pacific, San Diego, California, U.S.A.*

Keywords: Cybersecurity Investment, Acquisition, Decision Support, Return on Cybersecurity Investment.

Abstract: Appropriate cybersecurity investment is a challenge faced by both private and public organizations. This challenge includes understanding the actual vulnerabilities of an organization's networked systems, as well as the cost of a successful cyber attack on those systems. On top of this, an organization's cybersecurity acquisition workforce must be able to discern reality from the marketing hype that is produced by cybersecurity sales forces. This paper builds upon earlier work which developed a cybersecurity acquisition decision support mechanism (Romero-Mariona. et al., 2016). In particular, cybersecurity technology evaluation results are extended to assist organizations to define a Return on Cybersecurity Investment. This new capability is instantiated within the context of networked critical infrastructure and industrial control systems.

1 INTRODUCTION

Cybersecurity is a complex challenge for many organizations, ranging from individuals surfing the Internet to public and private organizations. Many organizations, both public and private, have fallen victim to cyber attacks (Davis, 2015; Cieply and Barnes, 2015). Moreover, as Internet-connected systems are integrated more and more into the average person's daily life, cyber attacks have become a normal aspect of modern life for many people. Many attacks are of little to no consequence, however many attacks end up becoming high-visibility and costly cyber incidences, which may cause lasting damage to the organization. There are a variety of reasons that an organization's network may be susceptible to a cyber attack, ranging from personnel with poor online practices to systems that do not patch vulnerabilities in a timely manner. Cybersecurity investment is another challenge for organizations. Indeed, "cybersecurity investment" deals with multiple challenges including underinvestment, lifecycle management, etc.

Cybersecurity for organizations that own and operate cyber-physical systems—specifically industrial systems, critical infrastructure, or other legacy systems—is an especially challenging problem due to the fact that these systems often comprise of components that were not designed with security or modern interconnectedness in mind. For countries in conflict with an unscrupulous adversary, networked critical infrastructure systems can make an enticing target. Indeed, cyber attacks against critical infrastructure are well known to lead to severe consequences (Liang et al., 2016), as energy system disruption can lead to critical systems (e.g.,waste processing, hospital/medical systems, traffic lights,refrigeration/storage systems, etc.) failing. Even in countries that are not in active conflict, many critical infrastructure systems are known to be vulnerable to cyber attack and adversarial actors may have already compromised those systems (US-CERT, 2018).

To address these challenges, we developed the Resilient Critical Infrastructures through Secure and Efficient Microgrids (ReCIst) project, funded through the United States' Office of Naval Research Energy System Technology Evaluation Program (ESTEP)[1], to develop a decision-support capability that provides visibility into the true costs of introducing cybersecurity solutions to industrial power grids. The de-

[1]https://www.aptep.net/partners/estep/

Hallman, R., Major, M., Romero-Mariona, J., Phipps, R., Romero, E. and Miguel, J.
Return on Cybersecurity Investment in Operational Technology Systems: Quantifying the Value That Cybersecurity Technologies Provide after Integration.
DOI: 10.5220/0009416200430052
In *Proceedings of the 5th International Conference on Complexity, Future Information Systems and Risk (COMPLEXIS 2020)*, pages 43-52
ISBN: 978-989-758-427-5

cision of what cybersecurity solution would be best is ultimately a financial decision, therefore we developed a return on investment model to help acquisition workers navigate the costs of their own facilities in comparison with the costs and benefits associated with a virtual marketplace of potential cybersecurity solutions. Our main contributions in this paper are as follows:

- We build upon earlier work, which developed a decision support framework for a cybersecurity acquisition workforce (Romero-Mariona. et al., 2016) by feeding technology evaluations into a framework for determining a Return on Cybersecurity Investment (ROCI);
- We describe an instantiation of the ROCI model to quantify the effects of cybersecurity investment for critical infrastructure.

To the best of our knowledge, ours is the first cybersecurity investment framework that attempts to quantify a return on investment for the critical infrastructure sector.

The remainder of this paper is organized as follows: Section 2 provides surveys previous work on cybersecurity investment strategies and cybersecurity economics. Our cybersecurity technology evaluation and decision support framework is reviewed in Section 3. Section 4 describes the Return on Cybersecurity Investment model within the context of industrial control systems and networked critical infrastructure while Section 5 demonstrates the feeding of technology evaluations to determine a ROCI for the adoption of a suite of cybersecurity technologies. Concluding remarks and ongoing/planned work is found in Section 6.

2 RELATED WORK

The challenges of optimizing an organization's cybersecurity investment is reasonably well studied. Some organizations (e.g., large companies, governments, etc.) may be able to support a specialized cybersecurity workforce which serves as a center of institutional knowledge and can provide direction or assistance on the issue throughout the organization. If in-house cybersecurity expertise cannot be maintained, cybersecurity strategies for investment and network management must rely on other knowledge bases (e.g., internal personnel with some level of cybersecurity knowledge, vendor sales teams, etc.). Beyond the initial investment in cybersecurity technology, there are a host of other issues which must be taken into consideration. Some of these issues include workforce development and continued certifications and lifecycle management for integrated cybersecurity acquisitions.

2.1 Cybersecurity Investment Strategies

Gordon and Loeb developed a cybersecurity investment model that has become the seminal work on the subject (Gordon and Loeb, 2002). The Gordon and Loeb model deals with information technology rather than operational technology systems, specifically focusing on protecting information sets. The model shows that organizations should not necessarily focus cybersecurity investments on the most vulnerable information sets, which may be exorbitantly expensive to protect, instead investing on the protection of information sets with intermediate-level vulnerabilities. Additionally, the model gives instruction on optimization, suggesting that an organization only needs to spend a small fraction of the expected loss from a cyber attack.

Further work from Gordon, Loeb, et al., build upon their original model. (Gordon et al., 2014a) present a discussion on the different cybersecurity investment strategies that for-profit firms may pursue, as opposed to strategies pursued by non-profit organizations or governments. (Gordon et al., 2014b) takes external factors into account for determining how much an organization should optimally spend on cybersecurity investment. In particular, taking externalities into account, they showed that an optimal cybersecurity investment increases by at most 35% over the earlier investment model. Analysis on information sharing between organizations and the effect on cybersecurity investment—specifically avoiding underinvestment—is covered in (Gordon et al., 2015).

Cavusoglu, Mishra, and Raghunathan (Cavusoglu et al., 2004) present an explicit outcome-based cybersecurity investment model that attempts to calculate a return on security investment for IT systems. Their model utilizes Bayesian modeling and a game theoretic approach to inform which parts of a network are vulnerable to attack and how much manual monitoring should be implemented in order to minimize security cost. The model is applied to suites of cybersecurity technologies and optimized to direct specific acquisitions.

As with the Cavusoglu model, Quantitative Evaluation of Risk for Investment Efficient Strategies (QuERIES) (Carin et al., 2008), proposed by Carin, Cybenko, and Hughes, adopted a game theoretical approach to provide a computational approach to cybersecurity risk assessment. QuERIES was meant to deal with protecting IT systems that hold critical intellec-

tual property (IP) in which the loss of a single IP copy would prove catastrophic (e.g., weapon designs held in a military's network, personally identifiable information). Specifically, the QuERIES methodology is used for assessing the efficacy of network protections to prevent reverse engineering attacks. Given a model of an organization's security strategy, reverse engineering attack graphs are built and represented as Partially Observable Markov Decision Processes. Given these models, QuERIES provides optimal cybersecurity policies and investment.

Different organizations will have hold a variety of risk management strategies, (Huang et al., 2008) consider a cybersecurity investment strategy for risk-averse firms. This strategy is similar to the risk-neutral model (Gordon and Loeb, 2002), though it incorporates a different set of assumptions and boundary conditions. Under the assumption that not all cybersecurity risks are worth defending against, this strategy proposes some minimum possible loss as a trigger for cybersecurity investment, though the optimal level of cybersecurity investment does not necessarily increase with a firm's risk aversiveness. interestingly, they show that optimal investment will increase vulnerability.

Moore, Dynes, and Chang (Moore et al., 2015) interviewed security managers and executives (usually a Chief Information Security Officer or Chief Information Officer) across a series of sectors, including finance, healthcare, retail, and government organizations. These interviews demonstrated that most organizations rely heavily on frameworks to inform cybersecurity investment decision making [2]. Moreover, due to this reliance on process-oriented frameworks (Joint Task Force and Transformation Initiative, 2013), investment metrics that consider outcomes, such as Return on Investment, are not calculated.

3 EVALUATING CYBERSECURITY TECHNOLOGIES

Cybersecurity is a growing concern for governments around the world. The United States Government, for example, is on the receiving end of more than 100,000 daily cyber attacks (Maloney, 2016). Furthermore, Cybersecurity investment strategies must account for the reality that cybersecurity technology is a fast-growing market and constantly evolving to counter threats to information and operational systems. In spite of the fact that it spends billions of dollars annually on cybersecurity (Morgan, 2016), the United States Government lacks a standardized and repeatable methodology for evaluating cybersecurity technologies and informing investment strategies. As a consequence of this lack of standardization and repeatability, the acquisition process inevitably leads to duplicated efforts on the part of technical and acquisition personnel. Moreover, lessons learned within one sector of the Government are not easily shared with others, which may lead to multiple agencies adopting a cybersecurity technology that fails to meet their needs. In certain sectors of the government, where personnel are rotated through on a regular basis, cybersecurity policies and products may be changed with each shift in project supervision. A practical and important consequence of this is that cybersecurity acquisition decisions will be made by security non-experts. If an expert in a security topic leaves a team, their institutional knowledge on that topic may be lost to current personnel. Knowledge that was common sense in previous decision-making efforts is not obvious to new team members.

We developed a standardized and repeatable methodology for evaluating cybersecurity technologies, the DoD-Centric and Independent Technology Evaluation Capability (DITEC) (Romero-Mariona, 2014), to address these challenges[3] . DITEC provides a bulwark against the loss of institutional cybersecurity knowledge that is endemic to organizations where personnel are regularly rotated through, thus mitigating the risk of cybersecurity investment decisions being made solely by non-experts based on a sales presentation (Moore et al., 2015). Moreover, even when technical experts are given input in the cybersecurity acquisition process, they are likely to have biases that may not ideally suit the organization's local requirements. DITEC standardizes the cybersecurity acquisition process in part by instituting guidelines and frameworks, e.g., National Institute of Standards and Technology (NIST) Cybersecurity Framework, the DoD 8500 Series Information Assurance (IA) Controls[4], to establish the types of procedures, controls, threats, and features that provide the test cases for which cybersecurity technologies would be evaluated. A market survey was conducted to learn what technologies were available for acquisition and to classify them into a three-tiered categorization based on their capabilities. Technology evaluation metrics and a scoring algorithm were developed by creating a taxonomy which matched technologies and test cases, allowing users to evaluate and

[2]https://www.nist.gov/cyberframework

[3]Note that while DITEC is oriented for government use cases, it can easily be adapted to other organization models.

[4]https://www.stigviewer.com/controls/8500

make high-level comparisons of multiple technologies against one another.

3.1 DITEC Components

DITEC has three main components:

- The DITEC Process is used to evaluate a specific cybersecurity technology to determine how well it meets DoD/Navy needs;
- DITEC Metrics measure how well each technology meets the specified needs across 125 different test cases;
- The DITEC Framework provides the format necessary to compare and contrast multiple technologies of a specific cybersecurity area.

Cybersecurity technologies are rated by metrics on three levels of granularity. The highest level of granularity is the *Capability* level. There are 10 such Capabilities, which correspond to very broad ability categories (e.g., 'Protect', 'Respond', 'Operations', 'Lifecycle Management'). A middle level of granularity, *Sub-Capability*, narrows the focus from the Capability level (e.g., from 'Protect'—'Cryptographic Support', 'Lifecycle Management'—'Cost of Extended Vendor Support'). Finally, the *Sub-Capability Elements* level includes very specific test cases (e.g. Does the technology offer whitelisting?).

3.2 DITEC+

DITEC+ (Romero-Mariona et al., 2015) expands upon the initial DITEC proof of concept to implement the scalability required for further development and adoption, creating an enterprise-ready tool to aid in the acquisition process. Improvements on the initial DITEC concept include:

- Process–DITEC+ prescribes additional/customizable steps for focused evaluations pertaining to specific stakeholders and offers those steps as a library of evaluation guidelines;
- Metrics–DITEC+ revises and improves on the DITEC Metrics module in order to enable technologies to receive a "score" based on their evaluation performance against the metrics, providing the ability to apply "weights" to each evaluation per specific items of interest identified during the process, as well as support for prioritizing results based on a variety of different aspects;
- Framework–DITEC+ leverages the existing DITEC Framework but ensures that it is ready for enterprise-wide use, supporting multiple users and evaluations by adding robustness to the database and evaluation algorithms.

These and other improvements enable a DoD/Navy-centric, cost-effective, streamlined evaluation of various cybersecurity technologies, defined by a process that is standardized, flexible, repeatable, scalable, and granular metrics (developed in-house with subject matter expert support). Additionally, DITEC+:

- Supports multiple and concurrent users and technology evaluations;
- Provides the ability to compare various cybersecurity technology evaluations;
- Integrated CAULDRON (Jajodia et al., 2011), a network vulnerability mapping tool developed new metrics for measuring differences across evaluations and technologies while estimating the level of cybersecurity provided;
- Developed new metrics for measuring differences across evaluations and technologies while estimating the level of cybersecurity provided;
- Developed a new ranking/prioritization mechanism of evaluated technologies based on user preferences.

Recognizing that personnel at different levels of an organization would have competing priorities, the User Priority Designation (UPD) was developed to view evaluations in light of priorities. For example, an agency's comptroller may place a heavier priority on the lifetime cost of a product, where a network administrator would be more concerned with the ability to install a vendor update with minimal system downtime. Using DITEC+'s UPD tool, technology evaluations can be viewed by cybersecurity professionals and by management, allowing all stakeholders within the agency to project how various technologies and products will meet their needs according to differing criteria. Finally, to assist cybersecurity non-experts who have a role in the acquisition decision making process, we invented a recommender system which helps to match users to the technology (or suite of technologies) which best match their needs (Romero-Mariona et al., 2016).

3.3 Applying DITEC+ to Critical Infrastructures

The Cyber-SCADA Evaluation Capability (C-SEC) is an instantiation of DITEC+, designed specifically to test and evaluate the suitability of cybersecurity technologies to networked critical infrastructures, specifically Supervisory Control and Data Acquisition (SCADA) systems (Romero-Mariona. et al., 2016). Security has not traditionally been a concern

for SCADA systems because different manufacturers employed diverse protocols; however as protocols have become standardized this is no longer the case. Specifically, C-SEC utilizes the tools and processes of DITEC+ and applies them to a SCADA test bed, into which cybersecurity products are integrated and evaluated. The system receives a baseline vulnerability scan prior to product integration as well as a post-integration scan, the scans are then compared to determine the level of effectiveness based on an expected number of reduced vulnerabilities. Integration into the test bed system gives insight into how the product under evaluation (PuE) may affect other components in an operational environment. It also gives red team personnel the opportunity to stress test the test bed system with the PuE. To further demonstrate the effectiveness of the C-SEC approach, C-SEC On The Move mobilizes the DITEC+ infrastructure and the SCADA System scanner into a package that can be taken to SCADA system sites to run diagnostic scans, map vulnerabilities, and make recommendations for the acquisition and placement of cybersecurity products.

4 HIGH-LEVEL MODELING FOR A RETURN ON CYBERSECURITY INVESTMENT

The decision-making capabilities provided by DITEC+ and C-SEC's Technology Matching Tool (TMT) recommendation only serve to inform customers of the suitability of a solution based purely on the capabilities of that solution. Because of this, often the top ranked cyber solution recommendations in the C-SEC capability consistently include Security Information and Event Management (SIEM) solutions, SIEM capabilities typically include a broad spectrum of robust capabilities and consequently tend to be the most expensive. This can result in significant financial impact to not only procure, but to train and educate staff and weather downtime of industrial services during installation and routine maintenance. In the end, the decision to procure a cyber solution is a financial decision, where the decision to include cyber comes down to justifying the cost to procure, integrate, and maintain against the financial risks of a cyber attack.

The ReCIst capability improves on the previous cyber solution recommendation models by bringing the financial cost of integrating and maintaining a solution in line with the end user's financial picture. By focusing on the "is it worth it" aspect of cyber solutions, our Return on Cyber Investment (ROCI) model depicts how financial factors can measure the financial impact of a cyber attack, and how a cyber solution can mitigate - or contribute to - the financial fallout from a cyber attack.

The key features of ROCI borrow from typical return on investment (ROI) modeling.

$$ROI = \frac{AnnualLossExpectancy(ALE)}{CostofCountermeasure} * 100\%$$

where

$$ALE = (NumberOfPotentialIncidentsPerYear) * (PotentialLossPerIncident) * (\%Exposure)$$

In the ROCI model, the ultimate return value to determine whether or not procuring a cyber solution would result in a net gain or loss for an organization is calculated as the annual difference between costs associated with cyber attacks minus the costs of those same attacks, now mitigated by a cyber solution. Startup, training, and all up front costs, as well as annual maintenance for the cyber solution are included in the cost for cyber, as well as any impact to service, energy expenditure in particular. One of the main reasons organizations are hesitant to adopt cyber security technology in industrial systems is due to the availability of the industrial services taking the highest priority at all times. Taking systems offline to install and troubleshoot a cyber solution, and adding responsibilities for staff to maintain and audit this new solution, can be difficult to justify without financial incentive.

The full ROCI model is depicted in Figure 1 (Major et al., 2020). This model is depicted as a series of modular arithmetic calculations based off inputs which are sourced from customers, vendors, and research. Although many of the more abstract research values are still currently being discovered (e.g., average financial loss tied to social damage as a result of a publicized hack), even with a best guess, in the ReCIst software application a customer can evaluate the potential financial impact by adjusting risk inputs to determine a possible best or worst case scenario.

The ROCI model requires inputs of specific integer values from either the customer, the vendor, or publicly available data. The distinction is not made clearly at this time, as the source for these values may differ for each user of the ReCIst tool. Inputs include organization-specific values such as the hourly cost for services to be offline, which is expected during installation, testing, and maintenance. Labor costs are part of the model, including installation, testing, and maintenance, as well as training, troubleshooting, and

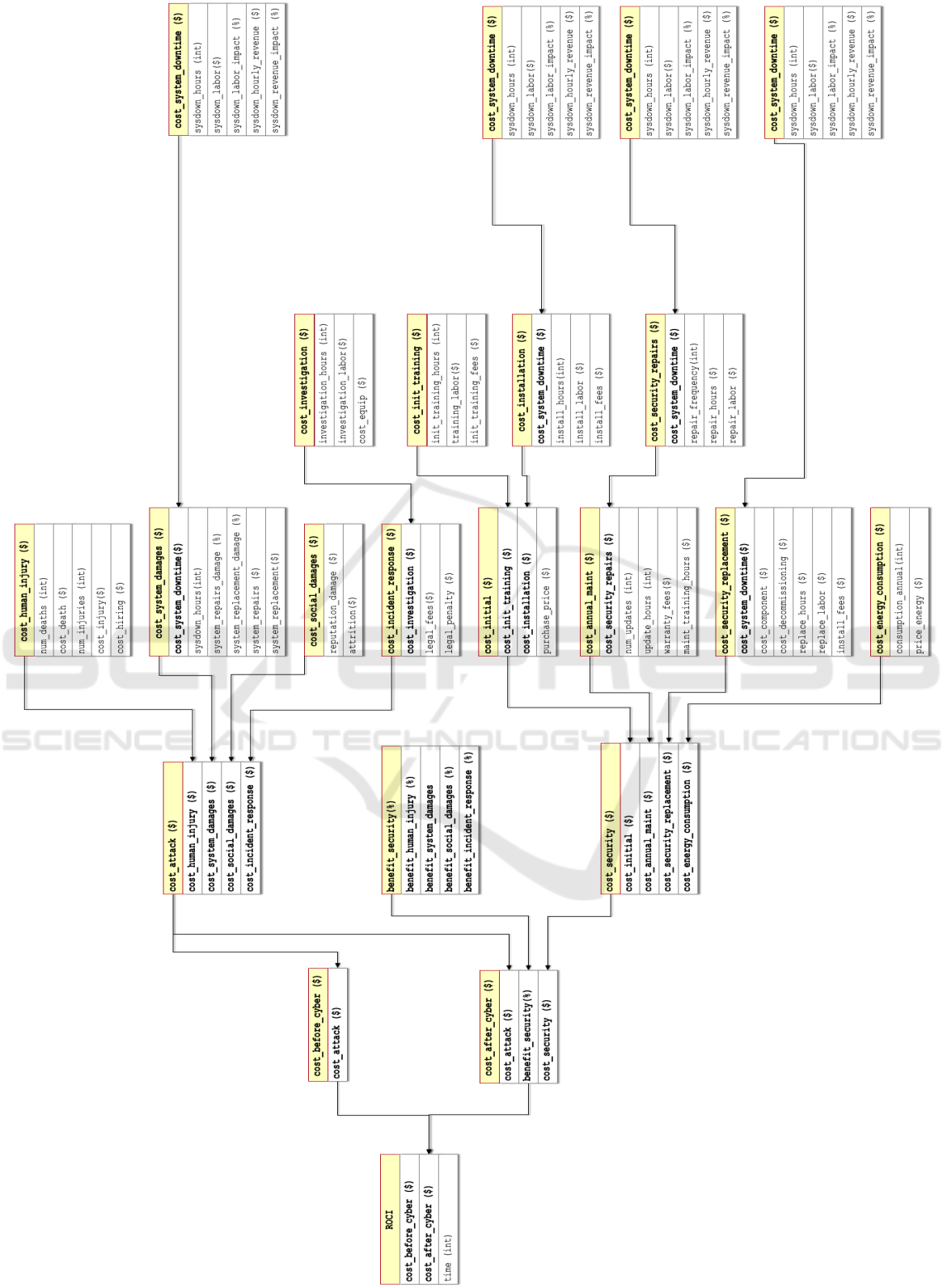

Figure 1: The Full Return on Cybersecurity Investment Model.

even the costs for auditing and forensics when a cyber attack does occur. The most difficult values to input into this model are those which can predict the likelihood and frequency of a cyber attack, as well as the scope of damage and recovery from such an attack. Other questions, which are more personal and customized to the organization include the financial costs associated with reputation damage when a leak is publicized.

These inputs are fed into a series of simple arithmetic calculations which in turn are used to calculate the ROCI score:

- `ROCI`
- `cost_before_security`
- `cost_after_security`
- `cost_attack`
  - `cost_human_injury`
  - `cost_system_damages`
  - `cost_system_downtime`
- `cost_social damages`
- `cost_incident_response`
- `cost_investigation`
- `cost_security`
- `cost_initial`
- `cost_init_training`
- `cost_installation`
- `cost_annual_maint`
- `cost_security_repairs`
- `cost_security_replacement`
- `cost_energy_consumption`
- `benefit_security` (currently simplified to a percentage of impact to each of the `cost_attack` values.)

It should be noted that the ROCI model is only used to calculate costs that can be directly attributed to to a cyber attack. Industrial systems often experience outages, downtime, and exhibit unexpected behavior due to normal events, such as equipment failure, mis-calibrations and human error, and even wildlife and other acts of nature. Intelligent industrial attacks which aim for low-key degradations of service - not openly destroy or cause outages - may not be diagnosed as a cyber attack for a period of time, if at all. While the ROCI model does not attempt to account for costs associated with variations in service that may or may not be part of normal industrial operations, it is possible that future versions of cyber investment models for industrial systems may use existing financial forecasting to supplement the ROCI value for solutions that detect or deter some percentage of these types of attack.

5 CALCULATING A RETURN ON CYBERSECURITY INVESTMENT BASED ON TECHNOLOGY EVALUATIONS

In the ReCIst tool, the ROCI model improves the C-SEC and DITEC+ recommendation capabilities to cyber solutions that also have the best ROCI value in addition to meeting customer needs. This integration is addressed in the following section.

The ReCIst capability integrates technology recommendations based on the user's technological needs, but then prioritizes the recommendations based on the best value ROCI score, presenting the top 3 to the user. See Figure 2.

Although this concept is simple in implementation - the top three technologies with the least financial impact are recommended - all the information gained can then be used to allow a user to re-prioritize and gain new recommendations based on the which aspects of each solution have the most financial impact. This gives the customer data which will empower them to make even better decisions based on their technological and financial goals.

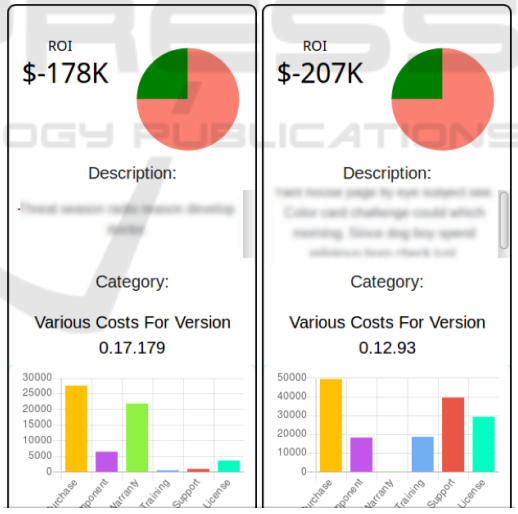

Figure 2: ROCI Impact Comparison for Two Products.

For example, ROCI data collected allows ReCIst to provide additional calculations for aspects such as total annual labor or system downtime costs. The ReCIst tool presents this information to the end user via a number of graphics. For example, in Figure 3, the first and third solutions are fairly well-balanced across categories, but the hardware cost is high, and energy costs low on the third option compared to the first solution, where energy costs are very high, and the hardware cost is average. If the customer is able to afford

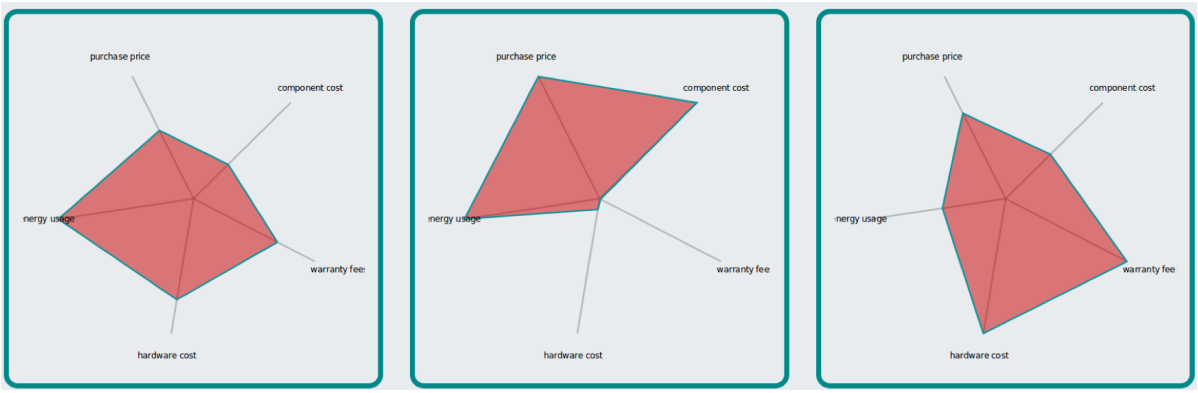

Figure 3: Radar Chart Depicting Cost Category Differences for Three Different Products.

a high up-front cost, but needs to keep recurring costs such as energy low, then the third option might be a better solution. If a given solution is only expensive because of initial startup and training fees, but if this product requires low maintenance fees and has a low failure rate, they may be willing to budget for a high startup cost, knowing the solution will pay for itself in the long run. While ROCI and the ReCIst capability focus on the first year of a solution - the decision to procure and the costs associated with the first year of a solution's life, future versions of this work will aim to incorporate forecasting, such as can be done in a fast-moving landscape of technological innovation and escalating cyber threats.

Users may also be able to mitigate some of these costs in-house. For example, if 100% system downtime is too financially impactful for installation and maintenance, but the customer has a strategy in mind, which involves only taking half of the systems offline at any given time, minimizing service disruptions, then they know that while their labor rates may rise during these times, the service impact to their customers is minimal, and in the end, they will gain enhanced cyber protections with minimal impact to reputation and customer turnover. These numbers can empower end users to make these kinds of decisions, whereas previously they might have been difficult to justify.

6 CONCLUSIONS AND FUTURE WORK

Cybersecurity is a complex and difficult challenge for organizations with Internet-connected systems. These complexities and difficulties are multiplied when legacy systems or operational technologies such as electrical generation and distribution infrastructure are Internet-connected, as earlier designers and engineers did not foresee modern interconnectedness or security risks. We introduce ReCIst, which integrates the output of our earlier work in cybersecurity technology evaluation and decision support frameworks to quantify a return on investment for cybersecurity technologies, specifically in the critical infrastructure sector. This is, to the best of our knowledge, the first attempt at examining the return on cybersecurity investment for critical infrastructure or other publicly-owned/managed, critical systems.

Our ReCIst capability aims to ease the burden of cyber solution decision-making for microgrid facility managers by producing a Return on Cyber Investment (ROCI) model, which considers not only the costs associated with a cyber solution, but how that solution's impact on the costs associated with a cyber attack affect the bottom line. The model is designed to be expanded, so that follow-on research and cost complexities can further optimize the decision making process.

Ongoing work includes:

- The inclusion of new inputs, such as results from a vulnerability scanner (e.g., Nessus) which are factored into a cyber vulnerability score;
- The inclusion of a recommender system (Romero-Mariona et al., 2016) which can assist an organization's acquisition workforce in optimizing their ROCI;
- Generalize the ROCI model beyond the current critical infrastructure instantiation, thus enabling the model's application to model the benefits of cybersecurity technology to all manner of networked systems;
- Improve the ROCI model to include the nuance of how specific cyber capabilities mitigate specific certain cyber threats or risks, so that solution capabilities are more accurately tied to financial gain or loss;

- Incorporate external impacts on ROCI such as cyber insurance;
- Forecasting long-term investment impacts which plan beyond the first year of cyber solution adoption, including equipment failure rates, annual maintenance, degradation of performance and technological upgrades;
- Model attack diversity and intended consequences that may map to military or government sites (do attack statistics show that different exploits are utilized for target-specific campaigns, such as data exfiltration compared to reduced mission effectiveness?);

Evaluating risk and risk management is another complex field of study. In the traditional two-axis management view of risk, risk calculation depends on two independent variables: consequence (the impact of a successful attack), and probability (the likelihood that the attack will be successfully executed). Currently, the ROCI model conflates these two variables, an action that may reduce the granularity of the model's analysis. In the future, ROCI may be improved by separating these axes, according to the traditional model of risk estimation. Furthermore, While cybersecurity risk has been modeled in the traditional risk management matrix (Collard et al., 2016), other research shows that these risk matrices are not effective (Thomas, 2013). Various research methods also exist to show that decisions can be optimized by incorporating risk (Hubbard and Seiersen, 2016). By capturing the nuances of risk and the methods used to manage the risk, the Return-on-Investment models and recommendations would be even more robust, giving system managers a greater amount of knowledge with where and how to improve their system from cyber attacks in a cost-efficient and effective manner.

ACKNOWLEDGEMENTS

Roger A. Hallman is supported by the United States Department of Defense SMART Scholarship for Service Program, funded by USD/R&E (The Under Secretary of Defense-Research and Engineering), National Defense Education Program (NDEP) / BA-1, Basic Research.

REFERENCES

Bergner., S. and Lechner., U. (2017). Cybersecurity ontology for critical infrastructures. In *Proceedings of the 9th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management - Volume 2: KEOD,*, pages 80–85. INSTICC, SciTePress.

Bodin, L. D., Gordon, L. A., Loeb, M. P., and Wang, A. (2018). Cybersecurity insurance and risk-sharing. *Journal of Accounting and Public Policy*, 37(6):527–544.

Carin, L., Cybenko, G., and Hughes, J. (2008). Cybersecurity strategies: The queries methodology. *Computer*, 41(8):20–26.

Cavusoglu, H., Mishra, B., and Raghunathan, S. (2004). A model for evaluating it security investments. *Communications of the ACM*, 47(7):87–92.

Cieply, M. and Barnes, B. (2015). Sony attack, first a nuisance, swiftly grew into a firestorm. *The New York Times*, page A1. https://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html.

Collard, G., Disson, E., Talens, G., and Ducroquet, S. (2016). Proposition of a method to aid security classification in cybersecurity context. In *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, pages 88–95. IEEE.

Davis, J. H. (2015). Hacking exposed 21 million in u.s., government says. *The New York Times*, page A1. https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html.

Gordon, L. A. and Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, 5(4):438–457.

Gordon, L. A., Loeb, M. P., and Lucyshyn, W. (2014a). Cybersecurity investments in the private sector: the role of governments. *Geo. J. Int'l Aff.*, 15:79.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., and Zhou, L. (2015). The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy*, 34(5):509–519.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., Zhou, L., et al. (2014b). Externalities and the magnitude of cyber security underinvestment by private sector firms: a modification of the gordon-loeb model. *Journal of Information Security*, 6(01):24.

Huang, C. D., Hu, Q., and Behara, R. S. (2008). An economic analysis of the optimal information security investment in the case of a risk-averse firm. *International journal of production economics*, 114(2):793–804.

Hubbard, D. W. and Seiersen, R. (2016). *How to measure anything in cybersecurity risk*. John Wiley & Sons.

Jajodia, S., Noel, S., Kalapa, P., Albanese, M., and Williams, J. (2011). Cauldron mission-centric cyber situational awareness with defense in depth. In *2011-MILCOM 2011 Military Communications Conference*, pages 1339–1344. IEEE.

Joint Task Force and Transformation Initiative (2013). Security and privacy controls for federal information systems and organizations. *NIST Special Publication*, 800(53):8–13.

Liang, G., Weller, S. R., Zhao, J., Luo, F., and Dong, Z. Y. (2016). The 2015 ukraine blackout: Implications for false data injection attacks. *IEEE Transactions on Power Systems*, 32(4):3317–3318.

Major, M., Romero-Mariona, J., Phipps, R., Tacliad, F., Slayback, S. M., Romero, E., and Hallman, R. A. (2020). Towards quantifying energy resiliency through return on cyber investment modeling. In *HICSS Symposium on Cybersecurity Big Data Analytics*.

Maloney, M. (2016). Pentagon's dc3i memo acknowledges thousands of cyber breaches that compromised dod systems and commits to new cyber culture. *Governmentcontractinsider.com*.

Moore, T., Dynes, S., and Chang, F. R. (2015). Identifying how firms manage cybersecurity investment. *Available: Southern Methodist University. Available at: http://blog. smu. edu/research/files/2015/10/SMU-IBM. pdf (Accessed 2015-12-14)*, 32.

Morgan, S. (2016). Worldwide cybersecurity spending increasing to $170 billion by 2020. *Forbes.com*.

Omerovic., A., Vefsnmo., H., Erdogan., G., Gjerde., O., Gramme., E., and Simonsen., S. (2019). A feasibility study of a method for identification and modelling of cybersecurity risks in the context of smart power grids. In *Proceedings of the 4th International Conference on Complexity, Future Information Systems and Risk - Volume 1: COMPLEXIS,*, pages 39–51. INSTICC, SciTePress.

Romero-Mariona, J. (2014). Ditec (dod-centric and independent technology evaluation capability): a process for testing security. In *2014 IEEE Seventh International Conference on Software Testing, Verification and Validation Workshops*, pages 24–25. IEEE.

Romero-Mariona, J., Hallman, R., Kline, M., Palavicini, G., Bryan, J., San Miguel, J., Kerr, L., Major, M., and Alvarez, J. (2015). An approach to organizational cybersecurity. In *International Workshop on Enterprise Security*, pages 203–222. Springer.

Romero-Mariona., J., Hallman, R. A., Kline, M., Miguel, J. S., Major, M., and Kerr, L. (2016). Security in the industrial internet of things - the c-sec approach. In *Proceedings of the International Conference on Internet of Things and Big Data - Volume 1: IoTBD,*, pages 421–428. INSTICC, SciTePress.

Romero-Mariona, J., Kerr, L., Hallman, R., Coronado, B., Bryan, J., Kline, M., Palavicini, G., Major, M., and San Miguel, J. (2016). Tmt: Technology matching tool for scada network security. In *2016 Cybersecurity Symposium (CYBERSEC)*, pages 38–43. IEEE.

Sedgewick, A. (2014). Framework for improving critical infrastructure cybersecurity, version 1.0. Technical report.

Thomas, P. (2013). The risk of using risk matrices. Master's thesis, University of Stavanger, Norway.

US-CERT (2018). Alert (ta18-074a): Russian government cyber activity targeting energy and other critical infrastructure sectors. https://www.us-cert.gov/ncas/alerts/TA18-074A.

Woods, D. and Moore, T. (2019). Does insurance have a future in governing cybersecurity? *IEEE Security and Privacy Magazine*.