# Exploring the CyberSecurity Paradox and Community Response

David A. Wagle

School of Business, Northcentral University TIM-8301: Principles of Cybersecurity

Dr. Bill Souza April 18,2021

# Exploring the CyberSecurity Paradox and Community Response Introduction

When multiple parties are faced with opportunities to balance maximum shared outcomes with minimized personal harms, behavioral economics tells us that often

sub-optimal behaviors will arise spontaneously (Viscusi, [2015).](#_bookmark21) These irrational behaviors appear to be relatively universal to the human condition and are somewhat predictable (Ariely, [2010).](#_bookmark0) Such results are often the product of conflicting goals making sub-optimal choices individually rational with respect to risk management even though such choices are, at the group level, overtly irrational and even harmful. In cybersecurity, there exist a phenomenon where competing public and private interests complicate fighting cybercrime. Policing agencies want to work with victims and prosecute criminals; industry victims want to resolve their risk exposure and limit negative press; and researchers want to collect and analyze data in order to improve protections and enhance prosecutorial abilities

(Atapour-Abarghouei et al., [2020).](#_bookmark2) While all parties wish to see cybercrime prevented and cybercriminals prosecuted, each party finds that other parties resist cooperation. Industry victims wish to keep their data and information of the attack secret, or at least understated, so as to avoid negative press. Law enforcement wishes to keep details of the attack and methods secret so as to preclude copycat incidents. Researchers seek to keep data and information private so as to enable access to reluctant industry members. The result is that while all parties agree that sharing data is necessary to further their common goals, no party is ready (or sometimes able) to share their data with the others.

# The Problem of Data

For technology-based companies, data is effectively the basis of their product or service. As such companies are reluctant to share data with researcher. Healthcare sector companies, for example, specifically balk at sharing, citing concerns relating to ethics, data security, costs, and public relations (Pisani et al., [2019).](#_bookmark18) It is not only in healthcare where

such concerns limit data sharing, in the shipping industry, even while large companies such as Merck invest hundreds of millions into end-to-end blockchain supply chain management systems, smaller shipping companies refuse to invest in such technology due to a desire to refrain from sharing data (Papathanasiou et al., [2020).](#_bookmark17) The modern direction of cybersecurity threat detection is to utilize machine learning, particularly neural networks, in intrusion detection systems, to flag attacks. Modern AI driven IDS systems have quite high accuracy for positive identification of for some types of attacks, some exceeding 97%, however, they come with a false positive rate of nearly 10%, which greatly diminishes their overall utility. Still other types of attacks had a positive identification rate of only 56%, which is quite low (Larriva-Novo et al., [2020).](#_bookmark11)

Cybersecurity needs advanced AI techniques to keep up with the exponentially expanding attack surfaces presented by smart technologies and the internet of things. But the ability to create a truly robust machine learning model is dependent upon the availability of detailed data from confirmed attacks as well as data from confirmed

non-attack events. Lacking such robust data sets, developers risk “over-fitting” their models, leading to high false positives (Larriva-Novo et al., [2020;](#_bookmark11) Sarker et al., [2020).](#_bookmark20) This data should ideally include information about the company, metadata about the data itself, system configuration data, and other elements that most corporations consider highly confidential and proprietary. Therefore, a major hurdle to overcome in the cybersecurity space, both for practitioners, researchers, and companies is to develop a method for trusted sharing of proprietary data for cybersecurity use.

# Overview of Cybersecurity

Cybersecurity is a broad topic that covers a broad range of activities. Today, the general standard for cybersecurity is the US Government’s National Institute of Standards and Technology report CSWP 04162018, frequently referened to as the NIST framework (Shackelford, [2016).](#_bookmark22) This framework consists of a core set of activities, outcomes, and

references for common critical infrastructure sectors. The material is organized to allow for communication of the activities and outcomes across organizations from the “c-suite” to the lowest level operators (NIST, [2018).](#_bookmark16) The framework also provides a tiered method for evaluating the maturity of an organization with respect to the core activities.

The key framework functions are Indentify, Protect, Detect, Respond, and Recover.

Each of these functions has subcategories to outline the scope of the function.

# Identify

Under the Identify function are the categories of Asset Management, Business Environment, Governance, Risk Assessment, Risk Management Strategy, and Supply Chain Risk Management.

Within the communications and networking sphere, these strategies align with IT Service Management frameworks such as ITIL and COBIT (Debora Suryawan & Veronica, [2018)](#_bookmark5) with the exception of supply chain risk management. As these ITSM frameworks are frequently employed in larger communications and networking firms, addressing the NIST requirements for security in the networking and communications space for this function should focus primarily on ensuring that supply chain risk management is on par with the other categories. The emerging role of blockchain in supply chain management systems will do a great deal to facilitate supply chain risk management for all firms (Kshetri, [2018;](#_bookmark10) Min, [2019).](#_bookmark13)

# Protect

Within the Protect function are the categories of Identity Management and Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, and Proactive Technology.

This area is critical for communications and networking systems in particular because of the role that social engineering plays in gaining unauthorized access to data.

Data can be encrypted both at rest and in transit, all security maintenance patches can be applied, and there can be robust intrusion detection systems in place, but if a user gives away their login credentials, then an attacker’s job is basically complete. Indeed, while Awareness and Training is only one of the 23 total categories that are part of the NIST framework. However, social engineering attacks account for at least 50% of all cybersecurity breaches (Jeong et al., [2019).](#_bookmark9) Technology can partially address this weakness, for example by requiring multi-factor authentication. But understanding of how human behavior and psychology can be exploited to breech security measures remains an area where attackers seem to continue to outpace security professionals.

# Detect

The Detect function includes anomalies and events, security continuous monitoring, and detection processing.

In the computer networking space, these categories are more and more being addressed with artificial intelligence solutions (Sarker et al., [2020).](#_bookmark20) Detection of intrusion events, malware, network anomalies, and even software piracy using machine learning and deep learning have extremely high detection rates (Chaudhary et al., [2](#_bookmark4)020). However, challenges still exist as false positive rates often require significant human intervention for appropriate actions to be taken. Of particular interest for the communications and networking sector is the discovery of techniques that can successfully detect and act against attacks happening over encrypted data channels (Garcia et al., [2021).](#_bookmark6)

# Respond

The framework categories captured under response include Response Planning, Communications, Analysis, Mitigation, and Improvements. Once an event has been detected, it is important to respond to it appropriately. This starts with planning. For many companies, incident response is covered by their disaster response plan and business continuity planning. Problematically, in the author’s professional experience, many

businesses in the communications and networking space of paper-only plans. They very rarely, if ever, test their fail-over capabilities to ensure the validity of their plan because of fears of causing service disruptions. An area worth serious focus is bringing enterprise risk management and business continuity teams into closer alignment for most industries (Russo, [2019).](#_bookmark19)

Additionally, the culture of cybersecurity tends to be insular, and still largely values obscurity as a security practice. Thus, Communication is an area in need of serious focus. One recent study found that key obstacles in effective response are ensuring that employees are kept informed, the right people are seeing the right information, and different organizational functional areas collaborate with appropriate prioritization of actions (Ioannou et al., [2019).](#_bookmark7)

# Recover

Under recover, the NIST framework includes Recovery Planning, Improvements, and Communications. Similarly to response, cybersecurity culture means that communications are not always effective. Of critical concern is that bibliometric reviews of the available literature suggest that recovery planning is not an area of significant focus for researchers. In the healthcare industry, for example, a recent study found that only 3% of the publications studied touched on recovery planning (Jalali et al., [201](#_bookmark8)9). This, in spite of the fact that experts are in agreement that recovery planning is essential to effective recovery of a cybersecurity incident.

# General Observations

While cybersecurity receives a great deal of attention in the media and from researchers, it does not often receive the attention required from business leadership to successfully address the numerous problems that exist. Further, the rising rate of cybersecurity attacks across network and communication systems means that this lack of attention is bound to have serious consequences. In 2020, nearly 70% of businesses in an

Asia-Pacific survey suffered from a successful cyberattack, with 55% of the attacks being considered “serious” or worse. Despite this reality, cybersecurity budgets remain largely unchanged (N.A., [2021).](#_bookmark15)

Cybersecurity is a top-10 concern of IT management, and has been for at least a decade (Maurer et al., [2021).](#_bookmark14) However those same surveys show that for senior leadership, less than 36% consider cybersecurity a top concern in 2019. Only 52% of organizations surveyed include cybersecurity representatives in business strategy planning.

A famous talk given by Richard Clark, the then special adviser to the President on Cybersecurity at the RSA Conference in 2002 mentioned that the average firm spent less than 0.0025% of their corporate budget on cybersecurity, an amount that is frequently less than that spent on employee coffee (Lemos, [n.d.).](#_bookmark12) The results from the aforementioned Asia study demonstrates that the apathetic and indifferent attitude towards cybersecurity has not changed drastically over the years.

The recent events of the COVID-19 pandemic, which resulted in many companies moving to a remote-work paradigm should have highlighted the lack of security planning, budgets, and preparedness, which one would expect would drive senior leadership concern. However, the apathy towards spending money on cybersecurity remains nearly constant (N.A., [2021).](#_bookmark15) One plausible explanation for this phenomenon is the psychological phenomenon of psychological distance (Bendell et al., [2020).](#_bookmark3) The idea here is that because cybersecurity breaches are big, impersonal events, that are theoretical future catastrophes, and removed from leadership’s primary areas of personal responsibility, they seem highly improbable and thus leadership does not feel the psychological pressure to plan for them.

This is an unfortunate state of affairs, but it maybe addressed on grounds that do rise to the level of C-Suite engagement. First, cybersecurity deterence, prevention, and resolution can be driven through data-sharing models that meet the “intrinsic needs of business efficiency” (Wang et al., [2020).](#_bookmark23) Further, since the vast majority of successful cybersecurity breaches are initiated through human social engineering attacks, raising

employee engagement with regard to the nature of these attacks to a firms’ employee base can go a long way to securing the environment (Alshaikh & Adamson, [2021).](#_bookmark1) It should be noted that this is more than simply training on the nature of social engineering, which has been shown to be only moderately effective overall. Rather, it involves ensuring employees are psychologically attached to the goal of promoting and providing cybersecurity. While a challenge, it is not a challenge that requires massive budgets. But it does require engaged leadership.

# References

Alshaikh, M., & Adamson, B. (2021). From awareness to influence: Toward a model for improving employees’ security behaviour. *Personal and Ubiquitous Computing*, 1. <https://doi.org/10.1007/s00779-021-01551-2>

Ariely, D. (2010, April 27). *Predictably irrational, revised and expanded edition: The hidden forces that shape our decisions* (1 Exp Rev edition). New York, NY, Harper Perennial.

Atapour-Abarghouei, A., McGough, A. S., & Wall, D. S. (2020, November 20). *Resolving the cybersecurity data sharing paradox to scale up cybersecurity via a co-production approach towards data sharing*. Retrieved April 16, 2021, from <http://arxiv.org/abs/2011.12709>

Bendell, B., Sullivan, D. M., & Ornstein, S. (2020). How fear of "looming megacatastrophes" alters entrepreneurial activity rates through psychological distance. *Academy of Management Perspectives*, *.34* (4), 585–602. Retrieved April 18, 2021, from http://proxy1.ncu.edu/login?url=https://search.ebscohost.com/ login.aspx?direct=true&db=edb&AN=147296848&site=eds-live

Chaudhary, H., Detroja, A., Prajapati, P., & Shah, P. (2020). A review of various challenges in cybersecurity using artificial intelligence. *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), Intelligent Sustainable Systems (ICISS), 2020 3rd International Conference on*, 829–836. <https://doi.org/10.1109/ICISS49785.2020.9316003>

Debora Suryawan, A., & Veronica. (2018). Information technology service performance management using cobit and itil frameworks : A case study. *2018 International Conference on Information Management and Technology (ICIMTech), Information Management and Technology (ICIMTech), 2018 International Conference on*, 223–228. <https://doi.org/10.1109/ICIMTech.2018.8528197>

Garcia, N., Alcaniz, T., González-Vidal, A., Bernabe, J. B., Rivera, D., & Skarmeta, A. (2021). Distributed real-time slowdos attacks detection over encrypted traffic using artificial intelligence. *Journal of Network and Computer Applications*, *173*. <https://doi.org/10.1016/j.jnca.2020.102871>

Ioannou, M., Stavrou, E., & Bada, M. (2019, June). Cybersecurity culture in computer security incident response teams: Investigating difficulties in communication and coordination, In *2019 international conference on cyber security and protection of digital services (cyber security)*. 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). <https://doi.org/10.1109/CyberSecPODS.2019.8885240>

Jalali, M. S., Razak, S., Gordon, W., Perakslis, E., & Madnick, S. (2019). Health care and cybersecurity: Bibliometric analysis of the literature. *Journal of medical Internet* *research*, *21* (2), e12644. <https://doi.org/10.2196/12644>

Jeong, J., Mihelcic, J., Oliver, G., & Rudolph, C. (2019, December). Towards an improved understanding of human factors in cybersecurity, In *2019 ieee 5th international conference on collaboration and internet computing (cic)*. 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC). <https://doi.org/10.1109/CIC48465.2019.00047>

Kshetri, N. (2018). 1 blockchain’s roles in meeting key supply chain management objectives. *International Journal of Information Management*, *39*, 80–89. <https://doi.org/10.1016/j.ijinfomgt.2017.12.005>

Larriva-Novo, X. A., Vega-Barbas, M., Villagrá, V. A., & Rodrigo, M. S. (2020).

Evaluation of cybersecurity data set characteristics for their applicability to neural networks algorithms detecting cybersecurity anomalies. *IEEE Access*, *8*, 9005–9014. <https://doi.org/10.1109/ACCESS.2019.2963407>

Lemos, R. (n.d.). *Security guru: Let’s secure the net*. ZDNet. Retrieved April 18, 2021, from <https://www.zdnet.com/article/security-guru-lets-secure-the-net/>

Maurer, Kim, K., Kim, D., & Kappelman, L. A. (2021). Cybersecurity: Is it worse than we think? *Communications of the ACM*, *64* (2), 28–30. <https://doi.org/10.1145/3399667>

Min, H. (2019). Blockchain technology for enhancing supply chain resilience. *Business* *Horizons*, *62* (1), 35–45. <https://doi.org/10.1016/j.bushor.2018.08.012>

N.A. (2021). Cyberattacks rise while stagnant budgets & apathetic leadership remain major cybersecurity barriers in asia pacific & japan: Study. *CIO & Leader*. Retrieved April 18, 2021, from [https://go-gale-com.proxy1.ncu.edu/ps/i.do?p=](https://go-gale-com.proxy1.ncu.edu/ps/i.do?p=STND&u=pres1571&id=GALE%7CA657420567&v=2.1&it=r&sid=ebsco) [STND&u=pres1571&id=GALE%7CA657420567&v=2.1&it=r&sid=ebsco](https://go-gale-com.proxy1.ncu.edu/ps/i.do?p=STND&u=pres1571&id=GALE%7CA657420567&v=2.1&it=r&sid=ebsco)

NIST. (2018, April 16). *Framework for improving critical infrastructure cybersecurity, version 1.1* (NIST CSWP 04162018). National Institute of Standards and Technology. Gaithersburg, MD. <https://doi.org/10.6028/NIST.CSWP.04162018>

Papathanasiou, A., Cole, R., & Murray, P. (2020). The (non-)application of blockchain technology in the greek shipping industry. *European Management Journal*, *38* (6), 927–938. <https://doi.org/10.1016/j.emj.2020.04.007>

Pisani, A. R., Kanuri, N., Filbin, B., Gallo, C., Gould, M., Lehmann, L. S., Levine, R., Marcotte, J. E., Pascal, B., Rousseau, D., Turner, S., Yen, S., & Ranney, M. L. (2019). Protecting user privacy and rights in academic data-sharing partnerships: Principles from a pilot program at crisis text line. *Journal of medical Internet* *research*, *21* (1), e11507. <https://doi.org/10.2196/11507>

Russo, F. (2019). Connecting the disaster dots: The benefits of enhanced collaboration between business continuity and risk management. *Journal of Business Continuity & Emergency Planning*, *12* (3), 277–285. Retrieved April 18, 2021, from http://proxy1.ncu.edu/login?url=https://search.ebscohost.com/login.aspx?direct= true&db=bth&AN=135613401&site=eds-live

Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020).

Cybersecurity data science: An overview from machine learning perspective. *Journal of Big Data*, *7* (1), 41. <https://doi.org/10.1186/s40537-020-00318-5>

Shackelford, S. J. (2016). Business and cyber peace: We need you! *Business Horizons*, *59* (5), 539–548. <https://doi.org/10.1016/j.bushor.2016.03.015>

Viscusi, T. G. a. W. K. (2015, March 30). *Behavioral public choice: The behavioral paradox of government policy*. Brookings. Retrieved April 16, 2021, from [https://www.brookings.edu/research/behavioral-public-choice-the-behavioral-](https://www.brookings.edu/research/behavioral-public-choice-the-behavioral-paradox-of-government-policy/) [paradox-of-government-policy/](https://www.brookings.edu/research/behavioral-public-choice-the-behavioral-paradox-of-government-policy/)

Wang, Q.-H., Miller, S. M., & Deng, R. H. (2020). Driving cybersecurity policy insights from information on the internet. *IEEE Security Privacy*, *18* (6), 42–50. <https://doi.org/10.1109/MSEC.2020.3000765>