Overlooking the Little Guy: An Analysis of Cyber Incidents and Individual Harms

by

Rebecca Spiewak

B.A. International Relations, and Psychology
Tufts University (2013)

Submitted to the Institute for Data, Systems, and Society
in partial fulfillment of the requirements for the degree of

Master of Science in Technology and Policy

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

May 2022

Author ……..
Institute for Data, Systems, and Society
May 12, 2022

Certified by ……..
Daniel J. Weitzner
3Com Founders Principal Research Scientist
MIT Computer Science and Artificial Intelligence Laboratory
Thesis Supervisor

Certified by ……
Taylor Reynolds
Technology Policy Director
MIT Computer Science and Artificial Intelligence Laboratory
Thesis Supervisor

Accepted by ……
Noelle Eckley Selin
Professor, Institute for Data, Systems, and Society and
Department of Earth, Atmospheric and Planetary Sciences
Director, Technology and Policy Program

Overlooking the Little Guy: An Analysis of Cyber Incidents and Personal Harms

by

Rebecca Spiewak

B.A. International Relations, and Psychology
Tufts University (2013)

Submitted to the Institute for Data, Systems, and Society
On May 12, 2022, in partial fulfillment of the
requirements for the degree of
Master of Science in Technology and Policy

Abstract

Over the last decade, cybersecurity threats have drastically increased in scale, impact and frequency across the United States. As a result, companies and governments require active monitoring of their cyber risk. While cyber risk management frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework are helpful, in practice this framework is actualized through formalized approaches to cyber risk measurements. While the emphasis on entity-level loss is valuable in the continued fight against cybercrime and acts of cyberterrorism, the individual-level impact is often neglected, to the detriment of everyday users of vulnerable technologies. Negative impacts to individuals *as an outcome of* organizations being hacked are often not captured today, thereby artificially excluding costs to individuals from loss calculations.

Through this body of research, we propose a novel approach to size negative externalities in relation to cybersecurity incidents. In contrast to prior research, this approach emphasizes the harm experienced by individuals rather than financial losses to enterprises. We present a new Taxonomy of Individual Cyber Harms, a formalized harm assessment methodology, and a cyber risk forecasting model to predict probable estimates of individual harms through a series of Monte Carlo Simulations. Through the analysis, we show that not only do harms exist for individuals as a result of cyber incidents, but that the extent of this harm is sizeable and can be greater than the harm to the entity for specific types of cyber incidents. Our results demonstrate that harms to individuals make up 42% of total losses experienced due to cyber attacks on US municipalities, or an additional 72% of harms currently captured. From a policy perspective, a discussion follows providing recommendations for avenues for remedy and redress for individuals who have experienced harm from cyber attacks.

Acknowledgements

I truly could not have completed this work without the seemingly endless support and guidance from the dozens of smart, kind, and (extremely!) patient people in my personal, academic and professional lives. I would like to thank my advisor Daniel Weitzner, Director of the Internet Policy Research Initiative (IPRI), and Taylor Reynolds, Director of Technology Policy at IPRI for the lively discussions and ongoing research guidance throughout the year, helping me navigate the more economics and policy-oriented spaces related to cybersecurity. It is bittersweet that I decided to join IPRI a year into my Master's program, but I thank you both for welcoming me with open arms.

Thank you to Professor Lawrence Susskind in the MIT Department of Urban Studies and Planning (DUSP) for the fantastic opportunity to work on the public sector side of cybersecurity, which ultimately helped to inform the scope of my thesis.

I would like to thank my fellow security and privacy policy enthusiasts for the engaging discussions, and for giving me an escape from all of the climate and energy talk (sorry, MIT TPP friends), with a special shout out to Rui-Jie, Kevin, and Avi. And thank you to Saba for providing a constant stream of humor throughout the research process.

I would like to acknowledge my previous manager, JF Legault, for his continued mentorship and belief in me over the years, as well as for being a bottomless wealth of ~~caustic~~ perspectives on all things security.

A big thank you to my mom, dad, sister and papa for allowing me to ~~vent~~ talk about my research progress. I believe pretending to know what a thesis is for my sake may be the truest form of love and support.

Thank you to KRRAAY, Maggie and Jing for all of the zoom sessions, phone calls, and brief escapes that gave me strength during the pandemic and peace of mind throughout my research. In return, I promise to not disappear for two years again.

Thank you to my wonderful partner Benjy, who took on the immense role of TA and thesis sounding board in addition to housemate and partner. He wrote beautiful things about me in his thesis Acknowledgements section, which now can't be used in his vows. I will not make the same mistake (Look at him, continuing to teach me!).

Table of Contents

Introduction

Over the last decade, cybersecurity threats have drastically increased in scale, impact and frequency across the United States. From well-funded industries such as financial services and pharmaceuticals, to resource-constrained local governments, entities are experiencing an ongoing onslaught of attempted infiltration by malicious actors, with a staggering number resulting in a successful security breach [1]. In the last quarter of 2021 alone, organizations attempted to deter over 900 attacks per week, a 50% increase over the same period in 2020 [2]. These malicious actors are compelled to attack US entities due to a variety of drivers, including financial, geopolitical and reputational motives. Threat actors often are emboldened by the ease of exploiting an environment given the increase in attack surfaces and the exploit toolkits readily available [3], as well as the apparent lack of repercussions faced by successful attackers due to insufficient legal safeguards and a highly digitized, often anonymized financial system that increases the odds of profiting [4] [5]. Even in the face of demonstrable investments in technology controls, and adoption of cybersecurity best practices by both public and private organizations, society's dependency on a distributed population of heterogeneous technologies makes effective prevention and deterrence of cyber threats difficult to achieve [6].

From cyberterrorism to theft of sensitive personal data, cybersecurity risks vary widely [7]. To better capture and subsequently manage this diverse set of cyber-related consequences, security experts, policy-makers and operational risk stakeholders created relevant risk taxonomies, evaluation frameworks and quantification methodologies [8] [9] [10]. Although these risk management tools are valuable and leveraged today by many,

significant barriers exist to achieving a robust, more unified risk management framework. Security complexities, sector nuances, and the diversity of professional backgrounds within the security industry all contribute to and perpetuate this issue [11][12]. For example, while the White House signed an executive order in 2021 mandating all companies that sell to the government follow minimum security requirements, there is no single, mandatory standard across private institutions for evaluating and measuring their cybersecurity risk [13] [14]. Viewed all together, there is a need to overcome these challenges in order to achieve a more targeted, unified, and readily available cyber risk management toolkit, with an emphasis on meaningful measurements.

Diversity of Cyber Risk Management Audiences

While consistent standards, frameworks, and clear risk measurements are important to better manage and mitigate the impact of cyber attacks, it is important to acknowledge the differences in consequences and potential harm amongst victims – and therefore, a need for framework flexibility. For example, nations are concerned about national security and stolen intellectual property, while companies are more focused on the impact of an attack to their bottom-line [8]. Individuals differ as well, in that they wish to avoid more personal risks, such as identity theft and inter-personal reputational harm [7]. Differentiating how different categories of cyber attack victims are impacted is essential to ensuring appropriate attack mitigation techniques and cybersecurity policies are crafted with real audience needs in mind.

Given these distinctions, most cyber risk frameworks are catered towards enterprises and government entities, rather than individuals. Orlando (2021) defines risk management as

enabling, “a system to cope with the effects of uncertainty on business activity” and this is especially true in the case of cyber incidents [15]. Firms therefore have a greater need to utilize formal frameworks and actively monitor cyber risk, while individuals often do not prioritize security until after they are affected by a cyber attack [16].

Research Motivation: Cyber Incident Impacts and Harms

Honing in on the “impacts” dimension noted above, there is a wealth of research and analysis on the measurable outcomes resulting from a security incident to an organization rather than an individual. This partially stems from the recent shift in threats from individuals or small businesses to Big Game Hunting (BGH), which targets larger, more well-resourced organizations, and more recently incorporates extorting victim entities for high sums of cryptocurrency [17]. While the emphasis on entity-level loss is valuable in the continued fight against cybercrime and acts of cyberterrorism, the individual-level impact is often neglected, to the detriment of everyday users of vulnerable technologies. As with organizations, individuals may be specifically targeted by malicious threat actors. According to the Federal Bureau of Investigation’s (FBI’s) 2021 Internet Crime Report, the top categories of crime affecting individuals include romance scams, email compromise, cryptocurrency scams, tech support fraud, and ransomware [7].

However, the data collected for these incidents are often limited to attacks that specifically target individuals, not institutions. Negative impacts to individuals *as a result of* organizations being hacked are often not captured today, thereby artificially erasing costs to individuals from loss calculations. This particular type of impact – one that results from the sale and use of technology products and services provided by an entity to its consumers or

residents – can therefore be classified as a negative externality (and one that is poorly documented at that) [18]. This erasure minimizes the actual harm experienced by individuals as a result of an attack on a company or government. Without the ability to better name, acknowledge, and measure notions of loss and harm, there are few avenues for recourse or redress. Therefore, we feel an individual's experience of harm as a result of a cyber attack on an entity is an area worth investigating further through additional analysis of cyber incident loss data.

Research Area of Focus: Cybersecurity Externalities Affecting Individuals

The remainder of this work will focus on investigating two main areas, with the first serving as the primary research question of interest:

1. How can we better quantify negative externalities related to cybersecurity incidents, emphasizing the harm experienced by everyday individuals rather than the monetary, reputational, or proprietary data loss to enterprises?
2. What frameworks, measurements and policies can be leveraged to better provide individuals with mechanisms for effective remedy or redress in the event of a cybersecurity incident?

The first section will provide background regarding current concepts of cyber risk, impact, and harm based on existing literature. We then interrogate gaps in the literature in relation to acknowledging and sizing negative externalities from cyber attacks, leading to a hypothesis that individual harms from cyber attacks exist, are non-negligible in size, and are largely ignored by cyber risk quantification efforts. A new Taxonomy of Individual Harms, as well as an individual harm assessment methodology are proposed. Leveraging real-world

incident loss data for cyber attacks against US cities and towns, we undergo a high-level quantification exercise using Monte Carlo simulations, comparing measures of harm when loss data for individuals is or is not included. Our results demonstrate that harms to individuals make up 42% of total losses experienced due to cyber attacks on US municipalities. This is an additional 72% of harms currently captured at the entity-level. Given this result, we then explore potential avenues for remedy or redress for individuals in the event of a cybersecurity incident beyond mechanisms that exist today, making a distinction between solutions that do or do not take into account stakeholder liability or precise harm estimates. We close with areas ripe for further data collection and investigation that support our proposed framework and quantification methods, highlighting the need for better accountability models for both entities and end-users.

Chapter 1: Literature Review – Cyber Risk, Impact, and Harms

To properly understand the value of cyber risk identification and management as a means of managing cyber risk-related harms, a review of existing, relevant literature is key. We will first provide an overview of how cyber risk is defined, documented, and utilized by both organizations and individuals. Then, we will move to a review of current conceptualizations of harm in a security context, and discuss how those conceptualizations either include or ignore harm to individuals.

1.1 An Introduction to Cyber Risk Frameworks and Principles

At the most basic level, cybersecurity risk is defined as the impairment or loss of confidentiality, integrity or availability of data, services or assets, otherwise known as the "C-I-A Triad" [19]. More detailed risk frameworks and security practices generally build off of the C-I-A Triad, leveraging the framework as a sort of foundational truth to describe and manage broad risk outcomes [20]. According to the security rating company BitSight, the purpose of a cybersecurity framework is to provide, "a common language and set of standards for security leaders across countries and industries to understand their security postures" [21]. Security rating firm SecurityScorecard notes that these frameworks, "provide a set of "best practices" for determining risk tolerance and setting controls" [22]. A fundamental concept here is that cyber risk is related to a loss of some sort, either wholly or in part, via exposure, destruction, or suppression of data, services or assets. Risk incorporates notions of "likelihood" and "impact severity" of an event occurring [23]. In this case, the "event" is a cyber attack on a targeted nation-state, organization or individual victim. Cyber risk management practices aim to identify and measure the probability and potential

ramifications of a cyber attack. A common cyber risk analysis methodology that borrows from operational risk evaluation methods is the Risk and Control Self Assessment, or RCSA [24] [25]. The RCSA identifies inherent risk levels of business processes without controls in place, and outputs the residual risk level based on the measured effectiveness of the implemented controls, relying on a risk matrix to score control effectiveness [24] [26]. By adhering to cyber risk frameworks, stakeholders can plan and prioritize implementing high-value preventive, detective, and responsive risk mitigation capabilities and processes to protect valuable assets from cyber threats [27].

On the surface, cyber risk measurement and management may seem straightforward, but the underlying complexities of the security landscape has led to sundry and often divergent lenses through which to understand and manage cyber risk. For example, one difference among control frameworks is the primary area of focus that informs how notions of risk are described and organized. For instance, some cybersecurity risk frameworks are organized around security controls, while others focus on cyber threats or vulnerabilities [22]. For reference, a security control, as defined by the National Institute of Standards and Technology (NIST), is a "safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements" [28]. Many controls-oriented cyber risk frameworks are leveraged to measure the effectiveness of those security controls at mitigating cyber threats based on the expected minimum deterrence capabilities. One cybersecurity framework centered around control is the Center for Internet Security (CIS) Critical Security Controls, which includes controls such as Data Protection, Account Management, and Data Recovery [29]. The CIS controls are evaluated using its associated

CIS Controls Self Assessment Tool [30]. The results of this type of control assessment effort can in turn inform an overarching cyber risk mitigation strategy [22]. For cybersecurity threats, one well-known framework is MITRE ATT&CK [31]. MITRE's ATT&CK framework breaks down the tactics, techniques and procedures (TTPs) commonly used by malicious threat actors to exploit vulnerable environments. Organizations often leverage MITRE to analyze the attack likelihood of the risk equation, as well as assess how well controls stack up against particular TTPs [22].

Another dimension by which cyber risk frameworks differ is the intended audience. While many risk frameworks are broad in nature, many are targeted to specific industries and purposes. For example, the HITRUST Cybersecurity Framework is meant for healthcare organizations to assess their data protection capabilities and meet healthcare-specific heightened compliance obligations [32]. The Payment Card Industry Data Security Standards (PCI DSS) is meant for financial institutions and lays out minimum security requirements related to cardholder data, such as how cardholder data should be stored and encrypted [22].

Although focus areas and sector audiences differ for cyber risk frameworks, there is a general trend for cyber risk frameworks to cater to enterprise-level audiences rather than to consumers. The Cybersecurity Framework (CSF) is one such framework geared towards entities rather than individuals. Developed by NIST, the framework is indeed widely leveraged by organizations across dozens of industries today, albeit to different degrees [33]. The CSF, "not only helps organizations understand their cybersecurity risks (threats, vulnerabilities and impacts), but how to reduce these risks with customized measures" [34]. Other well-known entity-level frameworks include the International Organization for Standardization (ISO) 2700 series, Control Objectives for Information Technology (COBIT),

as well as the aforementioned frameworks above, many of which reference other existing standards and risk measurement methodologies [22] [35, p. 101].

The primacy of enterprise-centered cyber risk frameworks over personal ones is apparent and unsurprising given both the need for firms to combat frequent cyber threats and the resources available to dedicate to securing an entity's assets. While the home networks of individual people may be targeted by malicious threat actors, the likelihood and scale of the threats are far lower than that of an organization or public entity given the potential value of a person's assets in comparison to a business or government organization; this is evidenced by the difference in the price of personal cybersecurity insurance versus the cost of insuring entire entities [36] [37]. In addition, studies show that individuals often neglect to actively assess their own security risks and may not care sufficiently about the issues a cyber attack may present [16] [38]. As stated on the Kudelski Security-run blog ModernCISO, "people are more likely to hold a grudge with a restaurant they had a bad experience with than the credit company who lost enough of their data for a criminal to commit identity theft" [38].

However, simply because individuals often lack desire and resources to assess their own cyber risk does not mean no tools or frameworks exist; a need still remains. Security researchers and public interest technologists dedicated to safeguarding consumers have attempted to fill this gap [39][40]. For instance, the Electronic Frontier Foundation (EFF) developed an approach for creating a personal security plan as part of their Surveillance Self-Defense Project [41]. EFF provides an inquiry-based process to review the value of one's own personal assets, the protections in place and areas of weakness, as well as the likely threats to digital information and associated assets [41]. This process is based on the concept of threat modeling, which is one method of assessing risk given adversary intent and

personal risk tolerance for loss, exposure, or destruction of assets [42]. Other relevant personal security risk assessment frameworks include the Factors Analysis in Information Risk (FAIR) Privacy risk framework, which focuses on personal privacy risks to individuals rather than entities [40], as well as recommendations by the Federal Trade Commission on Personal Information and Data Protections [43].

Despite the existence of the few personal cyber risk frameworks noted above, there remains a dearth of cyber risk analysis methods dedicated to individuals. Moreover, risk frameworks aimed at enterprises ignore risks to individuals *that were caused by* a successful breach of their organization's network. The assessments focus on risk to the institution directly, but avoid evaluating associated risks to their clients, end-users or residents. This is problematic because although, as noted above, individuals may not voluntarily focus on their own security risks, cyber threats aimed at entities may still result in consequences that significantly affect them. To elucidate how these consequences impact society, we review conceptions of harm, loss and impact in a cybersecurity context.

1.2 Conceptualization of Harms, Loss and Impact in Cybersecurity

From a digital security perspective, notions of "harm", "loss", and "impact", are intimately related, although the latter two concepts are more widely used by security professionals, especially in reference to risk measurement and quantification efforts. NIST defines cyber impact as, "The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability" [44]. Thus, "harm" can be viewed as the negative consequence itself,

whereas “impact” is the relative size of the consequence. A loss is a representation of that harm, and can include things like financial or reputational costs [45]. When organizations utilize the cyber risk frameworks and associated assessment methodologies detailed above, there is an emphasis on the type and size of potential losses to the business. Impact analyses help to further size the negative effects resulting from cyber attacks to better inform detection, prevention, and recovery strategies.

Overall, this notion of loss helps risk practitioners, security professionals, business stakeholders and individual consumers understand what may be at stake in the event a cyber incident occurs. Determining the scale at which this loss can and does occur is important for planning purposes and remediation efforts to minimize the magnitude of harm experienced [23]. This need to name and size the scale of losses resulting from a security breach has resulted in a rich, diverse body of work focused on the systematic quantification of cyber risk [10]. Typically, negative outcomes are quantified in monetary losses to institutions, although there is inconsistency amongst stakeholders regarding how costs or losses should be defined and measured – a fact that often manifests in deviations in the coverage for cyber losses from cyber insurance companies [46]. For example, in a 2018 report, The Council of Economic Advisors provided cost estimates for cybersecurity events using changes in stock prices post-event, but highlight increases in company investment in security solutions as well [19]. Other common losses include any extortion funds paid to bad actors, the cost of restoring lost data, and the overall value of funds directly stolen from an organization [36][45]. To sufficiently clarify the significance of and relationship between harm, loss and impact in the context of cyber risk, we now provide a brief review of cyber risk measurement methodologies.

1.2.1 Cyber Risk Measurement and Data Collection Methods

There are countless methods of various maturity and purpose that attempt to articulate and quantify cyber risk, although there is no single consistently adopted method to systematically measure cyber risk and size potential impact to victims of cyber attacks. Ruan (2017) highlights measurement limitations, noting that, "qualitative methods lack granularity, objectivity and ability to assist in cost–benefit analysis, while quantitative methods lack efficiency, statistical robustness and reliable asset valuation" [27]. While this may be the case, there are several basic components required for usable assessment and measurement methods. First, methods are typically grounded in their framework's taxonomies. A taxonomy is "a comprehensive, common and stable set of […] categories that is used within an organization," and in the context of cyber risk, it "facilitates a comparative analysis of an organization's risk over time" [47]. Taxonomies are typically mutually exclusive and collectively exhaustive within a bounded scope, and help standardize the way stakeholders discuss and similarly comprehend terms within a security framework [48]. In addition, taxonomies provide a meaningful hierarchy to structure complex terms and concepts; the NIST CSF, for example, organizes security controls around a framework for stages of a cyber incident – Identify, Protect, Detect, Respond and Recover [9]. Similarly, MITRE systematizes the ATT&CK framework into high level stages of the Cyber Kill Chain, and then breaks down those stages into underlying threat techniques used by malicious threat actors [31]. Measurements can then be tied to a given taxonomy, thereby supporting a comprehensive and easily digestible method of defining and sizing cyber harms and impact.

Another common component to assessment and measurement methods is the actual types of estimations related to cyber risk. In their book *How to Measure Anything in*

Cybersecurity Risk, Douglas Hubbard and Richard Seiersen define measurement as, "A quantitatively expressed reduction of uncertainty based on one or more observations" [23]. Some methods rely on translating risk measures to ordinal scales or rankings, such as the common 1-5 risk ranking or high-medium-low scale used in RCSA evaluations [23] [24]. More precise operational risk models aim to estimate risk exposure and quantify exact amounts or ranges of financial loss in dollars based on particular data inputs and assumptions related to cyber incidents [49][50].

While there is no set standard to measure the impact of cyber incidents, there are numerous well-established models that organizations leverage. One systematic, granular methodology focused on quantifying financial losses to an organization is the Factor Analysis of Information Risk, commonly known as the FAIR Model [51]. FAIR leverages a standardized information and operational risk taxonomy to analyze risk scenarios using a highly structured data collection and measurement process. The model estimates both loss event frequency and magnitude, bucketing loss magnitude into primary and secondary losses [24][51]. Primary losses refer to losses that are directly caused by the actions of a hacker, such as theft of funds from financial accounts, whereas secondary losses include downstream effects such as legal fines [52]. Primary and secondary losses can be referred to as "direct" or "indirect" loss in a broader sense beyond the FAIR Model.

Another widely-adopted cyber risk quantification concept is Value-at-Risk, or VaR, which is used for market risk measurements as well [27]. VaR provides a risk estimate for a probable range of financial losses to an organization given specific statistical risk parameters and security data. The end-product of the analysis typically bubbles up to a single number, which can be tracked and compared over time [53]. The FAIR Model is considered to be a

specific sub-type of Cyber VaR analysis [51]. Other VaR models include Erola et. al's (2022) Cyber Value at Risk (CVaR) systematic approach to predicting financial losses [54], and Orlando's (2021) proposal to incorporated unexpected loss events into Cyber VaR calculations [15].

Third party cybersecurity rating companies are major players in the cyber risk quantification space as well, providing expertise, frameworks and models that less mature companies may lack [55]. Cybersecurity ratings are defined as "a comprehensive and dynamic measure of how secure a vendor or product is against malicious attacks, informed by data and KPIs," and rely on a third party view of cyber risk based on externally-collected data [56]. Security rating firms include companies like SecurityScorecard, BitSight, and UpGuard, each of which leverage their own proprietary methods and models to quantify risk into a single numeric or alphanumeric rating [56].

A key dependency of risk measurement is data access and collection efforts. Models rely on data that is often imprecise, non-standard, and difficult to obtain. Company-specific cyber incident data are logically quite sparse given their high-risk, low frequency nature [57]. Limitations are compounded by the fact that firms often shy away from sharing loss information for fear of reputational risk ramifications [58]. This difficulty to obtain meaningful risk data has led to numerous mass data collection efforts, with the intent to investigate the patterns and extent around attack outcomes in order to prevent, deter and respond to cyber incidents. For example, the annual Verizon Data Breach Investigation Report provides statistics for over 5,000 confirmed breaches, detailing the number of attacks per sector, the types of assets targeted (e.g., bank accounts), and the aggregate dollar loss amount to companies by attack type [59]. The annual IBM Data Breach Report also provides

aggregate cost metrics and trend analysis given known financial losses to companies directly harmed by hackers [60]. The Massachusetts Institute of Technology's Internet Policy Research Initiative (IPRI) collects cyber loss data in relation to failed controls as part of their Secure Cyber Risk Aggregation and Measurement (SCRAM) initiative [61]. Real cyber incident data is collected from companies and municipalities via a secure multi-party computation platform in order to highlight the extent companies are suffering financial losses in relation to the maturity of their security environment [62]. Through the author's work on SCRAM as a member of IPRI, the difficulty of collecting and analyzing large quantities of cyber incident data to inform meaningful cyber risk measurements became quite evident, and helped inform the basis of this research.

Although extensive efforts are taking place to enhance the measurement of cyber risks, especially through the collection of incident loss data, substantial gaps remain. In particular, there is limited transparency into, or acknowledgement regarding, what is included or excluded from loss and impact analyses, which is an essential aspect of sizing harms and accurately estimating losses. Indirect costs are often excluded or hidden, to the detriment of potential cyber attack victims [63]. In fact, Deloitte studies estimate that hidden costs such as operational disruption or destruction, or the loss of company reputation, account for over 95% of overall costs to a business [64].

One such cost estimate exclusion is the harm to individuals as a result of a cyber attack, rather than to an organization's bottom-line. Both the literature and business practices tend to exclude how people are impacted as a result of a cyber breach. In part, this is due to the aforementioned prioritization of cyber risk management frameworks for organizations rather than consumers due to the real-world need for business or government entities to

manage a large set of diverse risks on an ongoing basis [8] [15]. In addition, this scope exclusion is a byproduct of the difficulty of associating a negative outcome to a specific cyber event. Like many negative externalities, demonstrating cause and effect remains challenging, such as when a victim of a data breach cannot prove they will be targeted by cybercriminals engaging in identity theft *because of* the data breach itself [65]. Given this exclusion of individuals in many cyber risk analyses, we now delve deeper into the specific notion of harm in a cybersecurity context. Up to this point, the terms "loss" and "harm" have been largely used interchangeably. In the next section, our goal is to highlight existing bodies of work pertaining to cyber harms through both organizational and human-centric lenses, showcasing the considerable gap in the literature in both naming and measuring cyber-related harms to individuals.

1.2.2 Cybersecurity and Individual Harms

At the most fundamental level, harm is defined as "physical or mental damage" [66]. In US law, harm is synonymous with "injury", in the sense that an injury, "is a harm suffered by a person due to some act or omission done by another person, and can generally give rise to a civil tort claim or a criminal prosecution" [67]. In a more colloquial sense, harm is often said to be "experienced," and therefore more associated with people rather than corporations or institutions. This may account for the relative lack of the use of the word "harm" in cyber risk management circles, which focus almost exclusively on the probability, size and scope of negative ramifications of cyber attacks to organizations [51]. "Loss" is often used in lieu of harm in the literature because of the known and measurable monetary implications of a cyber attack to a business or entity, although more broadly organizations can be victims of

cyber-harms in that the value of an asset, data, or service is reduced in some way via destruction, damage or exposure [8][68].

In recent years, several bodies of research have attempted to fill the gap of articulating the nuances of various cyber harms, moving beyond financial losses to organizations. In their paper *A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate*, Agrafiotis et. al. (2018) builds off of economics and criminology to establish a taxonomy of cyber-harms for organizations [8]. Through this work, the authors define cyber-harm as, "the damage that arises as a direct result of an attack conducted wholly or partially via digital infrastructures, and the information, devices and software applications that these infrastructures are composed of." [8]. According to their proposed taxonomy, cyber-harms fall into five main buckets: physical / digital harm, economic harm, psychological harm, reputation harm, and social / societal harm. Underneath these buckets are distinct sub-types of harm to organizations, such as reduced business growth, worry/anxiety from employees, and media scrutiny [8]. Another cyber harm taxonomy detailed in *Cyber Harm: Concepts, Taxonomy and Measurement* creates a Cyber Harm Model, inclusive of both a harm taxonomy and cyber risk assessment process, for the purpose of evaluating harm at the national rather than organizational level [68]. This taxonomy is broader and inclusive of the organizational-level cyber-harm taxonomy, and expands the taxonomy to include political/governmental and cultural harms as well, breaking down how individual, organizational, and property/infrastructure harms all inform national security interests [68]. Both of these taxonomies go beyond financial loss and reflect on the need to identify, measure, and mitigate more intangible harms that negatively impact society and organizations [8][68].

While both of these bodies of work do touch upon cyber harms to people, policy-makers and business leaders are the intended audiences outside of academia. These taxonomies also prioritize attacks aimed at institutions rather than individuals. To explore cyber harms more closely tied to victims who are targeted as individual people, we turned to the Internet Crime Complaint Center (IC3) Report issued annually by the Federal Bureau of Investigation [7]. The IC3 receives complaints reported by victims, identifies and publicizes threat trends and patterns, and works on near and longer-term remediation steps on behalf of the victim [69]. According to the 2021 report, the top five types of cyber-crime of more than 550,000 individual complaints were extortion, identity theft, personal data breach, non-payment/non-delivery and phishing/vishing/smishing/pharming [69]. Throughout the report, harm is measured in monetary losses.

Other areas of recent yet highly informative security harm research intended for individual people rather than institutions bring privacy threats and harms into focus. For example, Levy and Schneier (2020) detail the nuances of privacy threats in the context of intimate relationships, highlighting common threat attributes [39]. The privacy harms described in personal abusive or manipulative relationships are often not financial in nature, but rather focus on power dynamics and relate to physical, sexual or emotional abuse [39]. Citron and Solove (2021) interrogate the history of privacy harms based on existing legal precedent, arguing for a better mechanism to address the effects of privacy harms to individuals and society [70]. The authors create a novel typology of privacy harms to support their goal and include: Physical, Economic, Reputational, Psychological, Autonomy, Discrimination, and Relationship Harms [70]. A key driver for recognizing these distinct privacy harms is to ensure personal privacy protections can be upheld with violations legally

enforced, which is often a challenge given the burden of establishing a direct link between privacy infringement occurrences and negative impacts to individuals [70] [71].

While the limited literature that exists does touch upon cyber harms to organizations or harms resulting from attacks targeting individuals, there remains a significant gap when accounting for "indirect" costs. Specifically, the harm to individuals *as a result of* an attack on an institution is often either incompletely captured or entirely excluded from cyber risk identification and impact measurement methods altogether. For example, in the case of the annual FBI IC3 Report, the analysis ignores estimates of the cost to address or remediate the actualized harm itself [69]. In the FAIR Model, losses to individuals are pointedly omitted from cyber harm quantification efforts unless the loss also impacts the victimized organization in some way [72]. This is problematic because the spillover effects to individuals due to a company's vulnerable technology being exploited by hackers can be very real and extremely harmful. This is most starkly seen with regard to attacks on critical infrastructure. For example, the 2017 NotPetya cyber attack in the Ukraine brought down institutions such as banks, utilities and transport. It was estimated that the pharmaceutical company Merck lost an estimated $870 million, while FedEx lost $400 million, as part of a total $10 billion price tag in total losses [73]. However, aggregated cost estimates and assessed damages should not be limited to affected businesses and government entities. Notably, Ukrainian residents went without access to financial assets, critical resources like electricity, and the freedom to move safely and freely [74]. These are actualized negative externalities affecting individuals due to a targeted cyber attack, yet the emphasis on articulating risk and sizing harms in the context of institutions masks the true extent of harms experienced, as well as the full range of victims.

This omission of individual harms from cyber risk frameworks and associated loss calculations is a significant issue that requires attention from academia, operational risk stakeholders, policy-makers and the cybersecurity community. In light of this, we aim to make individual harms resulting from a targeted attack on entities more transparent. Similar to the privacy harms typology developed by Citron and Solove [70], our objective is to articulate a Taxonomy of Individual Cyber Harms to support the acknowledgement and measurement of negative impacts, with the overarching goal of informing a discussion on potential redress to victimized individuals. To achieve this goal, we now propose a structured approach for articulating and sizing cyber harms to individuals.

Chapter 2: Methods for Sizing Individual Cyber Harms

The creation of a structured approach to categorize and size individual cyber harms caused by attacks on entities is a first step to mitigating the effects of these injuries. Without recognizing the true size of aggregated risks, preparation and remediation planning for cyber attacks will remain insufficient. Ignoring the existence of a cost, or the true extent of a harm to individuals does not remove the issue, but rather leaves society worse off and prioritizes enterprise-level investments at the expense of implementing policies and acquiring resources that could help people in need. To support the assessment of individual cyber harms, we first propose a Taxonomy of Individual Cyber Harms, drawing upon the existing literature. We then propose two different approaches to estimating the size of cyber harms to individuals.

2.1 Individual Cyber Harms: Proposed Taxonomy

To help reverse the minimization of cyber incident harms to individuals, we propose a Taxonomy of Individual Cyber Harms ("the Taxonomy"). The Taxonomy leverages the harms laid out in Citron's and Solove's Typology of Privacy Harms [70], as well as Agrafiotis et. al.'s organizationally-focused Taxonomy of Cyber-Harms [8], with some adjustments. Modifications were made to account for where additional granularity in the taxonomy is or is not highly relevant. We therefore consolidated the relevant sub-types of Social and Societal Harm in the Taxonomy of Cyber-Harms with Physical or Digital Harm into a new category, named "Safety and Security", and included the Autonomy Harms detailed in the Typology of Privacy Harms into this aggregate category as well. We also removed discrimination and relationship harms from the Typology of Privacy Harms, given their minimal relevance in the context of downwind effects to individuals when entities,

specifically, are exploited. With these changes, we bucketed cyber harms to individuals into four main categories:

Economic Harms

This is the direct loss of monetary funds or benefits to an individual, or the theft of sensitive information that could provide a malicious actor with future access to said funds or benefits. Examples of cyber incidents that could result in economic harms are hacked bank account or identity theft as a result of a broader company data breach. Economic harms typically are more easily recognized and quantifiable because losses can be measured in dollars.

Safety and Security Harms

This type of harm refers to the loss of access to or disruption of critical services such as Emergency Medical Services, healthcare, public safety, or critical public works. Ransomware attacks on public institutions are good examples of incidents that often result in safety and security harms to individuals. A ransomware attack on the city of Baltimore in 2018 left the city without the ability to call 911, resulting in a significant safety risk to Baltimore residents in the event of an emergency [75].

Reputational Harms

Organizations are usually the focus of reputational harm, typically in reference to brand management and the potential loss of customers; this is not the case for this taxonomy [45]. Instead, reputational harms to individuals coincide with when sensitive or confidential information is released as a result of a cyber attack against an entity. Reputational harm is a byproduct of the damage to an individual's image in society, often resulting in personal or

professional fallout. The infamous Ashley Madison hack that exposed millions of cheating spouses to their friends, families and communities resulted in notable reputational harm [8]. Several politicians were caught up in the scandal, with many resigning [76].

Psychological Harms

Psychological harm is the trauma and mental anguish associated with the aftermath of a cyber incident, including the inability to trust, paranoia related to technology use, and severe anxiety. Some victims of cyber attacks suffer from Post-Traumatic Stress Disorder (PTSD) in the aftermath of an incident. Support services that help victims after critical incidents have reported an uptick in emotional trauma caused by cyber events and invasions of privacy [77]. Psychological harms are understandably difficult to measure given the impact is on a person's well-being rather than a person's wallet, and hacked companies or cyber risk professionals may not have access to information that could take this type of harm into account or translate the harm estimates into monetary losses [8]. In extreme cases, as was seen in the aftermath of the Ashley Madison hack, individual victims experienced such mental anguish that they took their lives [76].

2.2 Individual Cyber Harms: Measurement Framework

A main benefit of developing the taxonomy above, beyond acknowledging the existence of individual cyber harms caused by cyber attacks on institutions, is the structure the taxonomy provides to assess the extent of the harm itself. Leveraging quantitative and qualitative metrics can support comprehension and analysis that better inform future harm mitigation strategies [68]. To create meaningful metrics in this space, we propose dimensions

that aid in the estimation of individual losses laid out in the Taxonomy. We bake in a reasonable assumption that there is relationship between specific dimensions of an attack's outcomes, and the extent of harm felt by affected individuals. Based on the type of attack, these harm dimensions factor into how significantly or minimally a cyber incident can impact individuals; through an economic lens, this can be viewed as estimating a price tag for the negative externalities resulting from the technology and services an entity provides to consumers and constituents [18].

Through this assessment framework, we associated each of the Individual Cyber Harms with three distinct harm dimensions ("Dimensions") to help estimate the magnitude of individual harms resulting from an attack against an organization:

Individual right to or ownership of data, asset, or service impacted

In the US legal system, a harm or injury is often associated with an infringement on a right of some sort [70]. The American Enterprise Institute, a public policy think tank focused on democracy and human rights expounds, "Think of people's legal rights as forming a bubble around them. When a right is invaded, the law recognizes that as harm and offers appropriate remedies." [78] When a company is hacked, data, assets or services may be affected. Under current systems, the company rather than the affected customers are taken into account [72]. However, there are certain rights individuals have to those affected data, assets or services in other, more traditional contexts. Therefore, recognizing the relative level of ownership one has over these items based on precedent could help size the harm (although not necessarily take into account the liability piece – more on that later). For instance, we have a strong, unambiguous individual right to keep our social security number private, outside of

interactions with specific, mostly government-run services, and to maintain that a social security number is for personal use only [79]. In contrast, the right for a parent's child to attend school and access education uninterrupted is a bit more nebulous. In the US, while there is a general belief for and investment in the right to access free education, there is no explicit guarantee codified at the federal level [80]. Therefore, if a school is shut down as a result of a security incident, the harm estimated may be considered smaller in the context of individual rights. This dimension can also inform post-incident remedy to victims given its somewhat more legally-grounded considerations.

Irreplaceability of data, asset or service impacted

As a second dimension, the inability to easily substitute the data or asset in the event of an attack influences the amount of harm experienced by an individual. For example, one reason why identity theft can take 100-200 hours over six months to remediate on average is because some of the data is not replaceable, meaning once the information is compromised only risk-mitigating protections can be put in place [81]. The lasting harm or the loss experienced through time to remediate is therefore highly associated with the irreplaceable nature of that data. In another example, journalist Mat Honan was hacked in 2012 due to Apple and Amazon security flaws [82]. Photos of his child as a baby were erased, something that was of immense value to the victim and cannot be replaced [83]. In contrast, a compromised credit card number is highly substitutable since the victim can often simply use another one, and be issued a new number with relative ease by the issuing bank. Inability to access credit, which would be the main economic harm, may not occur.

Permanence of impact

The third harm dimension, permanence of impact, refers to the length of time an individual is affected by the attack. The longer a victim is impacted, the greater the potential harm. This concept is not dissimilar to long tail costs experienced by firms in the wake of a cyber attack; IBM's 2021 Cost of a Data Breach Report shows that, on average, 16% of an organization's total costs caused by a data breach occur two years or more after the attack took place [60]. For individuals, permanence of impact could be high for identity theft that goes unresolved, or if critical care is not received due to a cyber incident bringing down a hospital's network.

Along with these three harm dimensions, we included one additional "weight factor" that could amplify the extent to which these dimensions play a role in harm outcomes:

Level of interconnectivity of affected data, asset or service

"Interconnectivity" refers to technology dependencies or credential re-use. For companies, one reason why there is such a degree of worry about the ease of lateral movement on a flat network is that once a malicious actor gains access to one asset or area of the network, there is risk of movement to other, often more sensitive assets [84]. A high level of interconnectivity is also the culprit for supply chain attacks, as was seen in the 2020 SolarWinds hack, where over 100 enterprise customers were affected by a singular point of failure in the SolarWinds software update code [85]. This logic for enterprises can be leveraged for individuals as well. An email compromise resulting from a broader cyber incident likely affects the confidentiality and accessibility to other important personal accounts; in the Mat Honan case, his compromised email account gave the attacker the opportunity to access his Twitter and Apple accounts as well [83]. Stolen credentials also

may result in additional attacks if those credentials are reused, or are common enough to be affected by attacks that leverage credential stuffing techniques [86].

By leveraging the proposed Taxonomy of Individual Cyber Harms and the associated Dimensions, we aim to provide a framework and methods by which individual harms resulting from cyber attacks on entities can be identified, assessed and measured. Through this work, we can then help inform ways to reduce the unaddressed cyber harms experienced by people. To demonstrate the value of this measurement framework, we conducted an exercise to assess and size individual harms of individuals. In the next section, we lay out the assessment methodology to size individual cyber harms before delving into an analysis using real-world cyber incident data.

2.3 Proposed Assessment and Harm Sizing Methods

The purpose of this section is to define a step-by-step methodology for quantifying measures of individual impact not captured today by organizational-level loss data. Measuring cyber loss data to inform overall cyber risk and impact is a complex task, partially due to the sparsity of incident datasets [25]. The general practice of measuring low-frequency, high-risk events such accidents (e.g., a plane crash), or in this case cyber incidents, comes with significant limitations regarding how broadly one can generalize and apply the outcomes of a limited set of cyber attacks to risk measures [57]. To combat this gap, we look to accurately simulate cyber attacks by leveraging the attack and harm details in our data. We estimate the distribution of frequency of cyber incidents per year, as well as the size of entity-level and individual-level harms annually for a cyber insurance pool with a similar risk profile.

One sensible way of measuring this uncertain risk is through a series of random samplings to generate possible outcomes based on known data and reasonable assumptions. This is best accomplished through a series of Monte Carlo simulations. A Monte Carlo Simulation is defined as, "a model used to predict the probability of different outcomes when the intervention of random variables is present", and thereby "help to explain the impact of risk and uncertainty" [87].

Analysis Details

This analysis is grounded in the Taxonomy of Individual Cyber Harms and associated Dimensions described above. To conduct this analysis, we use cyber incident insurance claims data submitted by municipalities. We believe using municipalities as our basis for analysis comes with specific advantages. First, municipalities often have a publicly available budget for reference to help value losses. Second, cities and towns provide a diverse array of essential services to their residents, which means there is a higher likelihood that more harm types will be included within the dataset. Lastly, the authors are interested in analyzing a resource-constrained environment, so subsequent discussion regarding redress are based on realistic assumptions.

First, we bucketed incident data into the harm categories defined above based on the descriptions provided in the data: Economic, Safety and Security, Reputational, and Psychological. There is one additional category ("Uncategorized") for incidents that do not have an adequate amount of data to move forward in the analysis. Then, we further break down each harm type into Incident Outcomes, such as identity theft, or system shutdown due

to ransomware. This grouping supports additional analysis, comparing individual and entity-level harms systematically per capita.

Then, we ran a Monte Carlo experiment that simulates the number of successful attacks per year, sampling from a Poisson distribution based on the percentages of attacks bucketed into each of the Taxonomy categories. The Poisson distribution shows, "the number of events occurring in a given time period, given the average number of times the event occurs over that time period" [88]. This distribution is particularly helpful for assessing the probability of randomly-occurring, discrete, independent events that can be associated with a set rate of occurrence [89]. The rate of events multiplied by a set time period is called a rate-parameter, typically represented by lambda λ [89]. For reference, the standard equation for a Poisson distribution [89] is:

$$P(n \text{ events in an interval}) = e^{-\lambda} \frac{\lambda^n}{n!}$$

The summary output compares individual-level harms that are not captured today to entity-level costs. To achieve this, we produce a set of distributions, depicted visually via histograms and cumulative plots. The histograms align with the harm types within the Taxonomy. The outputs include:

- Distributions of the incurred losses to the city or town, by cyber harm type
- Distributions of the harm to individuals, by cyber harm type

To size the harm to individuals noted in the second bullet above, two methodologies are explored: Per Capita Bottoms-Up Measures, and Case Study-Based Measures.

2.2.1 Per Capita Bottoms-Up Measures

This methodology recognizes that the relationship between incurred losses at the entity-level and the harm experienced by individuals in the event of a cyber attack can be tenuous. For example, a police station may only have ten computers and two servers, and therefore the direct cost of remediation to the municipality may remain small. However, the harm experienced by a resident in danger, with no ability to contact the police during a time of need, could have little known relationship to the cost incurred. To combat this discrepancy, we leverage a new methodology that bakes in a per capita view of losses based on types of attacks, termed Per Capita Bottoms-Up Measures. The attack types, referred to as Incident Outcomes, underly the Taxonomy of Individual Cyber Harms. The ultimate outputs of this method is a formulaic evaluation of individual-level harms that can be compared to entity-level losses.

To use this method, each individual harm dimension should be evaluated via an inquiry-based method that serve as options to help quantify the loss for each incident. For example, if a cyber incident puts an individual's life in danger, the Value of a Statistical Life (VoSL) may be used to help quantify potential losses; currently, VoSL is approximately $10 million [90]. This would fall under the Irreplaceability dimension, as shown in the table below.

	Inquiry Process	Metrics
Right/Ownership	• What is the perceived value of the affected asset or record?	Market value, black market value
Irreplaceability	• What is the level of ease to use or access alternatives? • How many alternatives exist?	Willingness-to-Pay (WTP), Value of Life (VoSL)
Permanence	• Can the effects of the attack be fully remediated? • What is the opportunity cost?	Mean Time to Recover (MTTR)
Interconnectivity	• How many dependencies are there on the affected asset?	# of associated accounts or assets

Table 1: Inquiry Process of sizing individual harms

The metrics are then translated into set parameters and incorporated into a standard formula for individual harms, and shown below:

$$Individual\ Cyber\ Harm = \frac{\sum_{i=1}^{n}(f_i * \pi_i * v_i)}{population}$$

Variable	Description	Unit
n	Number of different Incident Outcomes that impact the harm to an individual	-
f	Frequency of event occurrence	Metric per interval of time
π	Actualized harm, serving as a weight factor on the value of affected assets. This is dialed up or down depending on the assumed degree of actual harm to individuals.	Typically a percentage
v	Full value of potential harm based on the affected assets	US Dollars
population	Scope of individuals affected by an attack	Persons

Table 2: Description of variables for Individual Cyber Harm formula

As an example, for a ransomware attack the formula could be used in the following manner after following the inquiry process:

- f is the number of days of a ransomware attack per year

- π is the assumed drop in productivity experienced as a result of systems shutting down
- v is the potential greatest value of harm – i.e., the value of the impacted assets

The results from the series of inquiries and input parameters for individual cyber harms are subsequently incorporated into the Monte Carlo model.

2.2.2 Case Study-Based Measures

In this alternative harm sizing exercise, it is assumed that the loss experienced by individuals is correlated to the loss incurred at the entity-level – e.g., an individual harm has a direct relationship to the organizational-level costs or the size of the breach. This is often true for data breaches, where the number of records leaked can be correlated with the number of customers affected (i.e., the individual) [60].

This method is called "Case Study-Based" because it is dependent on the documentation of losses for cyber incident case studies for both organizations and individual victims, and then determining a quantifiable relationship between the two via the harm dimensions. Note that this dataset of case studies and coded relationships between entity and individual-level harms does not exist, and would need to be created in order to leverage this method. That being said, we still find value in describing this harm quantification method, and running through the exercise with dummy data.

Through the collection of historical cyber incident data, this method analyzes the relationship between different types of Incident Outcomes, as mentioned previously (e.g., identity theft, breach of a hospital's Electronic Healthcare Records), the size of the loss to the

entity (e.g., dollars lost, number of records exposed), and the impact to individuals via the dimensions of individual harm and the weight factor (Right/Ownership, Irreplaceability, Permanence, Interconnectivity).

Incident Outcomes have different associations with Rights/Ownership, Irreplaceability and Permanence harm dimensions, and the weight of each of these dimensions in relation to the total cost to an organization therefore vary. For example, the Economic harm associated with credit card number theft rates is quite low on the Irreplaceability dimension because credit card numbers can easily be reissued. Therefore, the individual-level harm incurred as a percentage of total entity-level harm incurred would be low as well. Below is a table representation of the Case Study-Based Correlated Measures:

	Individual Cyber Harm Dimensions		
Harm Type	Right/ Ownership *R*	Irreplaceability *I*	Permanence *P*
Economical *Incident Outcome 1* *Incident Outcome 2* **…**	High % of entity-level harm incurred = R_1	Low % of entity-level harm incurred = I_1	Low % of entity-level harm incurred = P_1
Safety and Security	R_2	I_2	P_2
Reputational	R_3	I_3	P_3
Psychological	R_4	I_4	P_4

Table 3: Bottoms-up Individual Harm Calculation Methodology Options

For a broader analysis, a Monte Carlo Simulation can then be run for cyber incidents per year, with each simulation *N* producing the following, with *c* denoting the weight of interconnectivity:

$$N = Entity\ level\ loss\ incured * ((R_1 + I_1 + P_1) * c)$$

While this method has its advantages in principle, in practice the historical case study data is currently unknown. Although the required data is not available today, we feel that the proposed model is valuable enough to demonstrate use with synthetic data in the next section, with the hope that future data collections efforts will make the missing relationships available. The modularity and transparency of the model allows for incremental replacements of the dummy distributions.

Chapter 3: Applied Methods: Results and Analysis

3.1 Applied Methods Overview

Our analysis is scoped to focus on cyber incident insurance claims submitted by municipalities. In order to analyze this dataset, the author agreed with the relevant insurance stakeholders to keep the specifics around the insurance claims confidential in order to avoid additional risk exposure on the part of previously attacked cities and towns. Therefore, overarching details relevant to the analysis will be provided, but the locations, names and sizes of the municipalities included within the dataset will remain concealed. Specifically, we leverage claims data for municipalities located in the United States for incidents taking place between July 1, 2018 and January 31, 2022. These municipalities make up one distinct insurance pool, with cities with populations above 115,000 excluded by the insurance company to better balance the risk profile of the pool. There are 49 claims total, with coverage extended to 250-500 cities and towns.

Each of the 49 claims are categorized within the bounds of the Taxonomy of Individual Cyber Harms: Economic, Safety and Security, Reputational, and Psychological. This categorization is derived from the anonymized, general loss description provided with each insurance claim. A fifth bucket, “Uncategorized”, is included as well for incident claims that do not provide adequate information within the loss description to be appropriately categorized and leveraged for analysis. While we acknowledge that each cyber incident can and likely is associated with multiples types of harm from the Taxonomy, for ease of analysis we bake in a strict one-to-one relationship between each individual incident in the claims

data and the categorization within the Taxonomy. This limitation can be reviewed and addressed in future research efforts.

Given the focus on municipalities, we also highlight whether there was a public service impacted by the cyber incident. Public services include emergency services, school systems, and other fundamental public works typically provided by a city or town, and funded by taxpayers. Based on the incident description provided for each insurance claim, we further break down and group the data into Incident Outcomes, such as "Endpoint data destruction requiring recovery" and "Unrecovered stolen funds".

We estimated the dollar value of individual harm associated with each incident and incorporated it within the dataset. The loss is provided in per capita terms, serving as an apples-to-apples comparative analysis between entity-level and individual harms caused by a cyber attack targeting a municipality. The estimated dollar value of individual harm follows the Per Capita Bottoms-Up Methodology detailed in the previous section, meaning each estimate is grounded in the detail provided in the incident description and leverages the Individual Cyber Harm equation. The table below provides high-level details for how individual cyber harm calculations were determined for each loss event given the nature of the attack described, with particular attention given to the Incident Outcome. Note that these calculations assume a "moderate" scenario for the percentage of potential harm actualized, and these figures can be dialed up or down in magnitude depending on ingoing assumptions. A more granular view of the basis for the loss calculations, including source information, can be found in Appendix A.

$$Individual\ harm = \frac{\sum_{i=1}^{n}(f_i * \pi_i * v_i)}{population}$$

Loss Calculations: Safety & Security Harms to Individuals

		Frequency of Event	Actualized Harm Factor (Amount of asset affected)	Potential Harm (Value of asset)	Calculation for Individual Cyber Harm
	Incident Outcome	f_i	π_i	v_i	*Moderate Scenario*
1	Police Station – 911 system down	.00198 calls to the police per person in municipality population per day *d*	.000896 actualized harm factor applied in a moderate scenario, based on annual rates of violent crimes prevented while in progress	10 million, based on the Value of a Statistical Life (VoSL)	$= (.00198\,d) * (.000896 * \$10M)$
2	Police Station – All technology down, ex. 911	Number of incidents, multiplied by the # of days *d* over 365 days in a year	Assumption: Drop experienced in police productivity during attack *Moderate scenario:* 15% drop in productivity	Budget *b* is spent annually per capita on average on police force in a given US state	$= \left(\frac{d}{365}\right) * (.15 * b)$
3	Fire Department – Fire-related death	$3*10^{-8}$ deaths per person per day *d*	Assumptions: Across all scenarios, death occurred so no additional weighting is applied *Moderate scenario:* 1	10 million, based on the Value of a Statistical Life (VoSL)	$= (3*10^{-8}d) * 10^{7}$
4	Fire Department – Fire-related injury	$1.4*10^{-7}$ injuries per person per day *d*	Assumptions: Injuries of varying degrees inform a discounting of the VoSL figure *Moderate scenario:* 20%	10 million, based on the Value of a Statistical Life (VoSL)	$= (1.4*10^{-7}d) * (.2 * 10^{7})$
5	Fire Department – EMS + Hazardous Conditions	.00022 calls per person per day *d*	Assumption: Required assistance cannot be provided to aid in prevention of loss of life *Moderate scenario:* .0537 actualized harm factor applied in a moderate scenario	10 million, based on the Value of a Statistical Life (VoSL)	$= (.00022d) * (5.38 \times 10^{-6} * 10^{7})$
6	Fire Department – All technology down	Number of incidents, multiplied by the # of days *d* over 365 days in a year	Assumption: Drop experienced in fire department productivity during attack *Moderate scenario:* 15% drop in productivity	Budget *b* is spent annually per capita on average on fire departments in a given US state	$= \left(\frac{d}{365}\right) * (.15 * b)$
7	Sewage pumps station damage	Number of incidents = 1	Assumption: Degree of damage of sewage pump station may vary *Moderate scenario:* 50% damaged	\$20,000 per *sewage station pump*	$= \frac{.5\,(20{,}000 * \#\ of\ pumps)}{population}$

Table 4: Bottoms-up Individual Harm Calculations by Incident Outcome for Safety & Security Harms

Loss Calculations: Economic Harms to Individuals

		Frequency of Event	Actualized Harm Factor (Amount of asset affected)	Potential Harm (Value of asset)	Calculation for Individual Cyber Harm
	Incident Outcome	f_i	π_i	v_i	*Moderate Scenario*
1	Ransomware Attack shutdown systems	1 incident * # of days *d* of a ransomware attack over 365 days in a year	Assumption: Drop experienced in productivity of municipality services during attack *Moderate scenario:* 15% drop in productivity	Median annual property tax paid in state attack occurred, *t* Average number of people per household = 2.6	$= \left(\frac{d}{365}\right) * \left(\frac{.15t}{2.6}\right)$
2	General breach of municipality network	Assumption: Each day *d* represents 8 hours of working time 1 incident * 8 hours * # of days *d* to contain an attack	Assumptions: For every 10K of a municipality population, another employee is required for remediation *Moderate scenario:* Assumed number of employees needed, as stated above	Average hourly IT municipality employee salary *s*, based on the US state the attack occurs in	$= 8d * \left(\frac{1}{10{,}000}\right) * s$
3	Financial administration shut down	Assumption: Each day *d* represents 8 hours of working time 1 incident * 8 hours * # of days *d* to contain an attack	Assumption: Drop experienced in productivity during attack *Moderate scenario:* 15% drop in productivity	Amount spent annually per capita in the state of that claim on finance administration, *spend* per municipality population	$= \left(\frac{d}{365}\right) * (.15 * spend)$
4	Data breach, exposed PII	.00139 chance identity theft due to breach per person	Assumption: Discounting for likelihood that identity theft is caused directly by this breach or a previous breach *Moderate scenario:* 10% drop in productivity	On average, it takes 100 - 200 hours for an individual to recover from identity theft, so using a midpoint 150 hours Median hourly earnings in the US is $16.36 Median dollar value lost = $800	$= (1.39 * 10^{-3}) * (.1 * (150 * 16.36) + 800)$
5	Unrecovered stolen funds	Number of incidents, assuming 1 incident	Assumption: The amount of unrecovered funds is set and does not align with conservative/moderate/aggressive scenarios	The analysis spreads the risk across the entire population	$= \frac{stolen - recovered}{population}$
6	Municipality employee identity theft	Number of incidents, assuming 1 incident	Assumption: The attack on municipal employees reduces productivity to serve the municipality *Moderate:* Assumed average number of employee hours required, with no additional or reduced magnitude	Average hourly IT municipality employee salary *s*, based on the state the attack occurs in Number of employees affected, *e* On average, it takes 100 - 200 hours for an individual to recover from identity theft, so using a midpoint 150 hours	$= \frac{150 * s * e}{population}$
7	Endpoint data destruction, requiring recovery	Number of incidents, assuming 1 incident	Assumption: Degree of damage of hard drive may vary *Moderate scenario:* Midpoint of Potential Harm range	Average data recovery cost per asset *asset* is about $1,000	$= \frac{1{,}000 * asset}{population}$

Note: Calculations for 5-7 do not scale by population. The risk is still spread across a municipality's population, but does not cancel out with any figure in the numerator and therefore remains in the final equations in the last column.

Table 5: Bottoms-up Individual Harm Calculations by Incident Outcome for Economic Harms

Loss Calculations: Reputational Harms to Individuals

		Frequency of Event	Actualized Harm Factor (Amount of asset affected)	Potential Harm (Value of asset)	Calculation for Individual Cyber Harm
	Incident Outcome	f_i	π_i	v_i	*Moderate Scenario*
1	Sensitive information exposed regarding criminal behavior	8.25 * 10^{-5} arrests per person per day *d* of exposed police log data	Assumption: Degree of harm experienced by known sensitive information *Moderate scenario:* 2% affected	Assumption: Missed job opportunities, based on 2021 median annualized salary of $34,600 over the course of 7 years	$= \left(8.25 * 10^{-5} * \frac{d}{365}\right) * .2 * 242,200$

Table 6: Bottoms-up Individual Harm Calculations by Incident Outcome for Reputational Harms

Loss Calculations: Psychological Harms to Individuals

		Frequency of Event	Actualized Harm Factor (Amount of asset affected)	Potential Harm (Value of asset)	Calculation for Individual Cyber Harm
	Incident Outcome	f_i	π_i	v_i	*Moderate Scenario*
1	Impact to children's access to education	1 incident * # of days *d* of a ransomware attack over 365 days in a year	Assumption: Degree of student education affected may vary *Moderate scenario:* 50% affected	Assumption: 500 students per school $14.5K is spent per student annually by taxpayers	$= \frac{\frac{d}{365} * .5\ (14,500 * 500 * \#\ of\ schools)}{population}$

Table 7: Bottoms-up Individual Harm Calculations by Incident Outcome for Psychological Harms

As previously highlighted in the Methodology section, cyber incident data is notably sparse [25]. The 3.5 years' worth of cyber incident data only includes 49 claims, and therefore conclusions derived from this data requires additional efforts to better ground and analyze both entity and individual-level harms. By expanding the risk profile of the 49 claims to thousands of incidents via simulated data, we can forecast future loss ranges and distributions for municipalities; this information can be generalized to conduct risk-based cyber analysis and decision-making. This scenario-generation is produced via a series of Monte Carlo samplings [87]. The annual rates of different types of cyber incidents and loss amount of associated harms drive the rate variable of the Poisson distribution underlying the Monte Carlo models. We can then assess the size and shape of the distributions to inform perspectives on the extent of entity versus individual-level cyber harms on a per capita basis, providing visibility into losses missing from standard risk calculations. For reference, the simulation code, implemented in Python, can be found in the Appendix B.

3.2 Summary of Entity-Level Harms

First, we reviewed the quantity of incidents that fell into each Harm Type. Economic harms were by far the most prevalent, responsible for about 70% of incidents included within the dataset. Of the 35 incidents categorized under Economic harms, 14 involved monetary fraud. Several claims indicated fraudulent accounts or redirected direct deposits for municipal employees. Other notable incidents associated with Economic harms involved phishing and ransomware (10% each). In addition, 12% of incidents were categorized as causing Safety and Security harms. These harms were often associated with public services such as police stations, fire stations, and sewage treatment. Both Psychological and

Reputational harms were not common in the dataset, with only 2 instances and 1 instance, respectively. While these two types of harms may indeed occur less frequently than others, this sparsity of data also speaks to the difficulty of identifying and quantifying less tangible harms. Cyber insurance coverage typically aligns with monetary losses, and therefore the descriptions provided by the claims may be biased towards including language that focuses on Economic rather than Psychological or Reputational harm. Below is a summary of the dataset organized via the Taxonomy of Individual Cyber Harms:

Taxonomy	Incident Count	Percentage of Total
Economic	35	71%
Safety & Security	6	12%
Uncategorized	5	10%
Reputational	2	4%
Psychological	1	2%
Total	**49**	**100%**

Table 8: Incident Frequency by Harm Type

The entity-level losses incurred in dollars by the municipalities were more weighted towards Economic harms, which are responsible for 84% of total costs over the 3.5 years in in the dataset. Again, this is understandable – a city or town would be more likely to submit a cyber insurance claim in the event of an incident that generates financial loss.

Harm Taxonomy	Entity-Level Loss ($)	Percentage of Total
Economic	$1,378,692	84%
Psychological	$169,006	10%
Safety & Security	$95,209	6%
Reputational	$455	0%
Uncategorized	$0	0%
Total	**$1,643,361**	**100%**

Table 9: Entity-Level Loss by Harm Type

We drilled down a level further to gain a better understanding of the types of services impacted by cyber attacks given particular Incident Outcomes. Of the 49 claims, 29% were due to a general breach of a municipality's network and 12% involved identity theft of municipality employees. Attacks against police stations and schools accounted for 8% of the dataset each, with singular incidents against a fire station, library and sewage station pump present as well. Overall, the total cost incurred by all municipalities over 3.5 years is only ~$1.6M for the entire insurance pool. However, there is significant individual-level harm excluded from consideration, thereby minimizing both the amount of risk and the associated impact of cyber attacks on US municipalities and its residents. This speaks to the overall value of undergoing an additional exercise to assess personal harms in the form of losses at the individual level.

Total Claims by Harm Type & Incident Outcome	Incident Count	Percentage of Total
Economic	**35**	**71%**
General breach of municipality network	14	29%
Municipality employee identity theft	6	12%
Not applicable to individuals	5	10%
Endpoint data destruction, requiring recovery	3	6%
Ransomware Attack shut down systems	3	6%
Unrecovered stolen funds	2	4%
Data breach, exposed PII	1	2%
Financial administration shut down	1	2%
Safety & Security	**6**	**12%**
Police Station – All technology down, ex. 911	2	4%
Police Station – 911 system down	1	2%
Sewage pumps station damage	1	2%
General breach of municipality network	1	2%
Fire Department – All technology down	0.25	1%
Fire Department – EMS + Hazardous Conditions	0.25	1%
Fire Department – Fire-related injury	0.25	1%
Fire Department – Fire-related death	0.25	1%
Uncategorized	**5**	**10%**
Uncategorized	5	10%
Psychological	**2**	**4%**
Impact to children's access to education	2	4%
Reputational	**1**	**2%**
Sensitive information exposed regarding criminal behavior	1	2%
Total	**49**	**100%**

Table 10: Incident frequency by Harm Type and Incident Outcome

Note: Incidents that included more than one incident outcome were divided evenly amongst those outcomes in the incident count

Total Entity-Level Loss by Harm Type & Incident Outcome	Entity-Level Loss ($)	Percentage of Total
Economic	**$1,378,692**	**84%**
General breach of municipality network	$590,722	36%
Endpoint data destruction, requiring recovery	$508,761	31%
Ransomware Attack shutdown systems	$201,790	12%
Not applicable to individuals	$29,637	2%
Financial administration shut down	$25,000	2%
Municipality employee identity theft	$13,415	1%
Unrecovered stolen funds	$9,368	1%
Data breach, exposed PII	$0	0%
Psychological	**$169,006**	**10%**
Impact to children's access to education	$169,006	10%
Safety & Security	**$95,209**	**6%**
Police Station – All technology down, ex. 911	$78,432	5%
General breach of municipality network	$10,009	1%
Police Station – 911 system down	$5,783	0%
Fire Department – All technology down	$246	0%
Fire Department – EMS + Hazardous Conditions	$246	0%
Fire Department – Fire-related death	$246	0%
Fire Department – Fire-related injury	$246	0%
Sewage pumps station damage	$0	0%
Reputational	**$455**	**0%**
Sensitive information exposed regarding criminal behavior	$455	0%
Total	**$1,643,361**	**100%**

Table 11: Total Entity-Level Losses across municipality dataset

Note: Incidents that included more than one incident outcome were divided evenly amongst those outcomes in the Entity-Level Loss column.

Public Service Impacted	Incident Count	Percentage of Total
None	38	77.6%
Police	4	8.2%
School	4	8.2%
Fire Station	1	2.0%
Library	1	2.0%
Sewer	1	2.0%
Total	**49**	**100.0%**

Table 12: Count of Public Services Impacted by a Cyber Incident

Public Service Impacted	Entity-Level Loss ($)	Percentage of Total
None	$1,330,735	78%
School	$218,025	8%
Police	$84,669	8%
Library	$8,947	2%
Fire Station	$986	2%
Sewer	-	2%
Total	**$1,643,361**	**100%**

Table 13: Entity-Level Loss of Public Services Impacted by a Cyber Incident

3.3 Sizing of Individual-Level Harms

3.3.1 Per Capita Bottoms-Up Measures: Results

Based on the relevant literature and current risk calculation methodologies at the entity-level, we hypothesize that individual-level harms are not adequately captured in standard cyber incident loss estimates. We reviewed how sizeable individual-level harms are often missing from risk and impact analyses, thereby making it difficult for an individual to obtain redress or remedy for harms experienced. The objective of this exercise is to explore this hypothesis, demonstrating both the presence of, and the extent to which, individual-level harms are missing from the loss calculations for incidents targeted at entities. Note that while not all individual-level harms result in a dollar value of loss, the loss calculations are translated into dollar values in order to provide a basis for a like-for-like comparison between entity-level and aggregated individual-level losses.

Through our individual-level harm calculations leveraging the methodologies described in Section 3.1, our analysis highlights that the harm to people caused by cyber attacks targeting municipalities can be a significant ratio of entity-level harms for certain Incident Outcomes. First, we reviewed the total estimated Individual-Level losses by Harm Type and underlying Incident Outcome. In total, an additional $1.18M in harms to individuals were

captured via our estimations across the cyber insurance claims dataset. Economic harms are responsible for 46% of these losses, with ransomware accounting for a majority of the costs. Safety and Security harms make up 36% of total harms to individuals, with attacks affecting police stations resulting in almost all of the costs to individuals for this Harm Type. Psychological harms, which included two instances of attacks on schools, account for 18% of the losses, while Reputational harms remain below 1% of losses.

Total Individual-Level Loss by Harm Type & Incident Outcome	**Individual-Level Loss ($)**	**Percentage of Total**
Economic	**$543,719**	**46%**
Ransomware Attack shut down systems	$387,728	33%
Unrecovered stolen funds	$82,315	7%
Municipality employee identity theft	$35,100	3%
General breach of municipality network	$24,894	2%
Data breach, exposed PII	$8,621	1%
Endpoint data destruction, requiring recovery	$5,000	0%
Financial administration shut down	$61	0%
Not applicable to individuals	$0	0%
Safety & Security	**$422,002**	**36%**
Police Station – 911 system down	$345,502	29%
Police Station – All technology down, ex. 911	$61,126	5%
Sewage pumps station damage	$10,000	1%
Fire Department – All technology down	$4,438	0%
General breach of municipality network	$579	0%
Fire Department – EMS + Hazardous Conditions	$354	0%
Fire Department – Fire-related injury	$1	0%
Fire Department – Fire-related death	$0	0%
Psychological	**$218,493**	**18%**
Impact to children's access to education	$218,493	18%
Reputational	**$591**	**0%**
Sensitive information exposed regarding criminal behavior	$591	0%
Total	**$1,184,805**	**100%**

Table 14: Total Individual-Level losses across municipality dataset

To gain a better understanding of harms for each individual rather than in the aggregate, we then assessed per capita individual harms in comparison to entity-level harms. This exercise was conducted with the understanding that risk is being spread equally across a municipality's population; however, the author acknowledges that many of the losses described, such as ones that impact a children's access to education, may not be evenly dispersed across an entire city or town's population under real-world conditions.

Each cyber incident insurance claim is grouped by Incident Outcome and Harm Type, expressing the average per capita harm for each. A multiplier on entity-level per capita harms is included to help elucidate the relationship between the two levels of harms.

Through this exercise, we found that ransomware attacks exhibited a greater absolute dollar amount and magnitude of harm to residents of municipalities on a per capita basis than direct municipality losses, at almost double the amount of entity-level harm captured. Attacks on police stations were a significant driver of individual harms, totaling more than $20 per person over the span of time provided in the dataset, or just shy of $6 per person per year. Additionally, the attacks against schools resulted in an additional 1.3 times the entity-level loss. Both data breaches exposing PII and water pump station breaches resulted in an additional $0.23 and $0.53 per capita respectively based on the individual harm calculations, where no harm was documented previously.

Note that while unrecovered funds and municipality employee identity theft did result in a greater magnitude of individual harms per capita than the entity harms per capita, the main driver of the magnitude of harm is the underlying asset, not the population. While a multiplier is still provided in Table 15, this means that while resulting individual harms not captured is spread across a municipality's population, there is no *per capita link* between the

individual and entity level harms. For example, the loss derived from the amount of stolen funds unrecovered is evenly spread amongst taxpayers, but that total amount of harm is not expected to scale up or down whether or not there are more or less residents in the municipality; in fact, the more residents in the affected municipality, the lower the per capita harm value. This is noted for the calculations on lines 5-7 in Table 5 in section 3.1.

Harm per Capita by Harm Type & Incident Outcome	Individual Harm ($)	Entity Harm ($)	Multiplier
Economic	**0.99**	**2.54**	**0.39**
Unrecovered stolen funds	1.69	0.35	4.83
Ransomware Attack shutdown systems	17.04	8.87	1.92
Municipality employee identity theft	0.30	0.11	2.73
General breach of municipality network	0.09	2.25	0.04
Financial administration shut down	0.01	4.88	0.00
Endpoint data destruction, requiring recovery	0.21	21.71	0.01
Data breach, exposed PII	0.23	0.00	.23 : 0
Safety & Security	**3.62**	**0.94**	**3.85**
Sewage pumps station damage	0.53	0.00	.53 : 0
Police Station – All technology down, ex. 911	2.54	3.50	0.73
Police Station – 911 system down	17.74	0.59	29.87
General breach of municipality network	0.09	1.62	0.06
Fire Department – Fire-related injury	0.00	0.08	0.00
Fire Department – Fire-related death	0.00	0.08	0.00
Fire Department – EMS + Hazardous Conditions	0.03	0.08	0.36
Fire Department – All technology down	0.37	0.08	4.50
Reputational	**0.03**	**0.03**	**1.30**
Sensitive information exposed regarding criminal behavior	0.03	0.03	1.30
Psychological	**4.04**	**3.12**	**1.29**
Impact to children's access to education	4.04	3.12	1.29
Total	**$1.60**	**$2.22**	**0.72**

Table 15: Per capita harms by Harm Type & Incident Outcome, Individual-level vs. Entity-level
Note: Data is rounded to the nearest hundredth

The lack of inclusion of individual-level losses for attacks targeting institutions therefore artificially deflates loss estimates. This not only impacts the accuracy of risk-based decision-making from a cybersecurity perspective, but essentially causes affected individuals to remain invisible victims of cyber harms given the lack of acknowledgement of the size and

extent of the human impact. This is true even when the multiplier is less than 1; an excluded loss is still important to consider, even if the harm to the individual is lower than the harm to the entity, because any noted individual harm is still *additional* to what is being captured today. While the dataset is small, these general figures also can be leveraged in the future to help estimate the probable uncaptured individual losses on a per capita basis for an attack that falls under a particular Incident Outcome. The dataset can be built out further over time as relationships between individual harms and direct losses at the organizational level become more transparent.

Moreover, it is important to acknowledge the limitations of grounding generalizable insights in a sparse dataset representing high-risk, infrequent events [91]. There is a high-level of uncertainty and variance in risk outcomes for cyber incidents, and baking those uncertainties into cyber risk and impact quantification efforts allows for reasonable assumptions and insights to be made [10]. Therefore, before delving further into the drivers for the quantity of individual-level harms not captured, we perform an additional level of analysis by pulling out the attack patterns from the dataset. These patterns are used to simulate a much larger group of incidents with a similar risk profile, which can then be leveraged to determine the distribution of the quantity of individual level harms. This probabilistic approach better reflects the uncertainty around the specific loss values, yet still allows us to determine and assess the relative size of individual harms not captured by many existing quantification efforts.

3.3.2 Per Capita Bottoms-Up Measures: Simulated Cyber Incidents

In order to derive generalizable findings from the relatively small dataset to predict future loss ranges and distributions for municipalities, we leverage a probabilistic sampling method to simulate additional cyber incidents, expanding the dataset to 5,000 simulated cyber incidents with a similar risk profile to the claims submitted in the municipality cyber insurance pool. A Monte Carlo modeling exercise was conducted, leveraging a Poisson probability distribution curve as the basis for random sampling. The key variable that informs the distribution is the rate-parameter and represents the numbers of instances of an event occurring in a specific amount of time [89]. The taxonomy-bucketed dataset includes the frequency and costs for different types of cyber incidents over a set length of time. By taking the entity-level costs and per capita harms incurred over the course of the 3.5 years included the data, we can produce annual attack rate-parameters for each of the individual harms within the Taxonomy, and randomly sample from the generated Poisson distribution.

We plotted the annual loss rates associated with the simulated cyber incidents on a per capita basis across all Harm Types, as well as for Economic harms to demonstrate the utility of the simulations. Aggregated harms per year are spread across the pro-rated municipality populations affected in the dataset. A comparative analysis between the entity-level and individual-level harms further elucidates the potential benefits to this exercise.

The distributions reflect that annual rate of per capita harms from the 49 claims in the dataset. Figure 1 shows a median per capita entity-level harm of $0.63, compared to $0.45 for individual harms. This breaks down to a .71 multiplier on entity-level harms to produce individual-level harms, aligning well with the .72 multiplier across all harms in Table 15. For Economic harms, the annual median per capita entity-level loss is $0.73, whereas the individual-level annual per capita losses are $0.28. The multiplier on entity-level losses in

sizing related individual-level harms is .38, again aligning well with the .39 multiplier between economic and individual-level per capita harms provided in Table 15. While the probable ranges for these annual per capita harms are quite small, amounting to tenths of a cent, and follow a relatively normal distribution, once aggregated across all affected municipality residents the range of losses can vary by several thousands of dollars. This is notable for a budget-strapped city or town that requires adequately-resourced resiliency planning in the event of an attack.

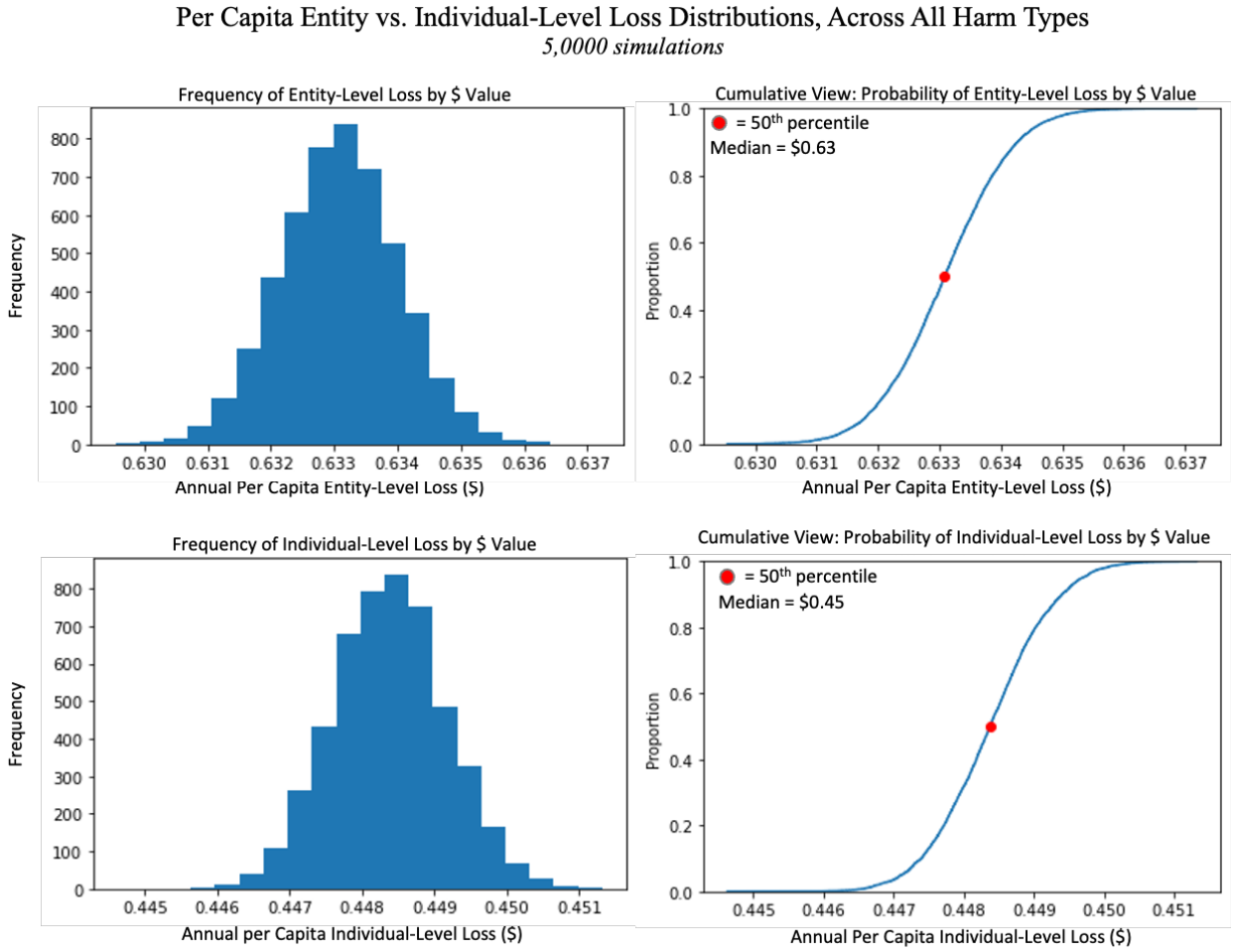

Figure 1: Annual Per Capita Entity vs. Individual Level Loss Distributions, All Harm Types

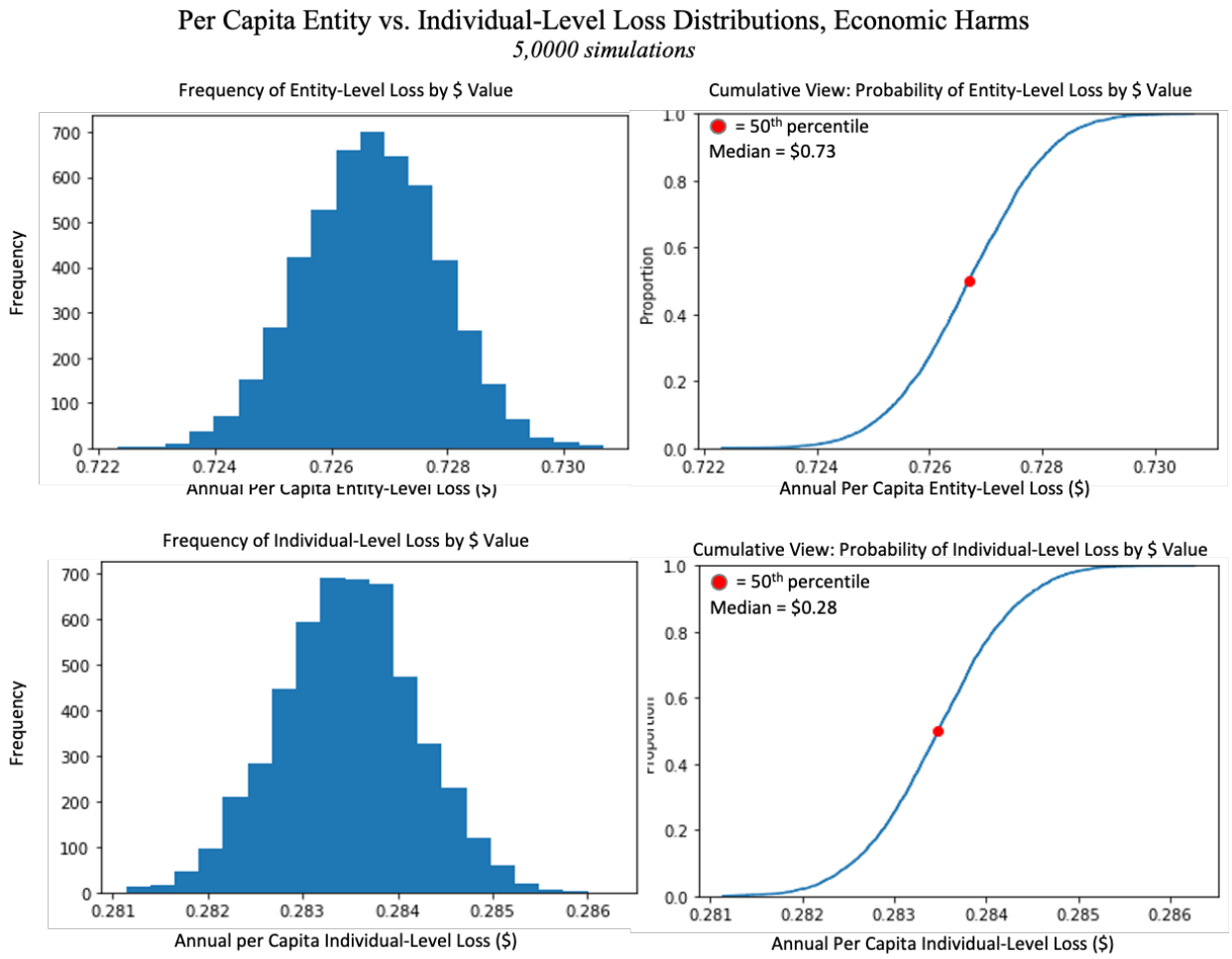

Figure 2: Annual Per Capita Entity vs. Individual Level Loss Distributions, Economic Harms

3.3.3 Drivers of Individual Harms

Upon reviewing the results of both the summary data and the simulation, a key question arises: Why are harm estimations for individuals so significant for certain types of attacks, especially in comparison to direct costs to municipalities? First, individual loss volumes are partially driven by the population of a city or town. Insurance claims typically account for finding and repairing the root cause of why the attack occurred in the first place; sometimes, the costs include any money paid out for extortion demands [92]. However, claims typically do not include the cost of an individual dealing with the ramifications of an attack, like

reversing acts of identity theft, and the magnitude of the harms from those types of attacks are directly proportional to the size of the municipality. Second, several of the claims in the dataset described ransomware attacks. The average length of downtime due to a ransomware attack in 2021 was 22 days, driving the costs related to the Permanence of Impact dimension up [93]. In addition, even though the estimated likelihood of loss of life was small for the attack scenarios present in the data, the "asset" the cost estimate is applied to is large – namely, the value of a person's life. As mentioned earlier in the chapter, the utilized Per Capita Bottoms-Up Methodology incorporates the Value of a Statistical Life (VoSL), which is about $10 million today [90]. This is an important takeaway -- the inability to access certain critical services, like calling 9-1-1 for emergency services, can present substantial risk to municipality residents. Even if the likelihood side of the risk equation is relatively small, the impact can be quite significant. This is one reason why the Cybersecurity and Infrastructure Security Agency (CISA) exists, to ensure critical infrastructure sectors remain resilient against cyber attacks, preventing harm to those living in the US [94]. However, this was not true across the board. The current likelihood of death or injury as a result of a fire-related incident has become so low that the individual harm calculations are negligible despite the underlying $10 million VoSL input for potential harm.

3.4 Alternative Harm-Sizing Method: Case Study-Based Correlated Measures

Additional research is required to build up a collection of historical incident data mapping the dimensions of individual harms – i.e., Right/Ownership, Irreplaceability, Permanence of Impact – to individual and entity-level costs. To accomplish this, first a set of descriptive cyber incidents impacting a particular sector would need to be collected and

tagged with the Taxonomy of Individual Cyber Harms. Each cyber incident would have an existing entity-level cost associated with it, likely from an insurance claim. Then, data would be organized into Incident Outcomes that fall under each Harm Type within the Taxonomy. After, the association of each dimension would need to be coded into the data. This information could be collected based on publicly available incident information, or via interviews with individual victims that serve as a representative sample. For example, during the May 2019 ransomware attack on the city of Baltimore, residents were unable to buy and sell homes while the applicable administrative software was shut down [95]. The affected victims could be interviewed and asked systematic questions related to their experiences and losses in relation to the dimensions outlined. After this dataset is built, a rough equation that estimates individual-level losses based on institutional costs can be created and leveraged for future estimates.

Using synthetic data, we forecast what a distribution of attacks causing individual harms could cost. We mock up synthetic data for the following Incident Outcomes associated with Economic harms:

		Dimension % of Entity Harm			Weight Factor
Incident Outcome	**Probability of Economic Harm in Dataset**	**Right/ Ownership**	**Irreplaceability**	**Permanence**	**Interconnectivity**
Credit Card Number Theft	25%	2%	0%	.5%	5
SSN Theft	75%	7%	5%	2%	10

Table 16: Synthetic data for Attack Profile Harm Dimensions, as a percentage of entity-level costs

We then run 5,000 simulations, sampling from the Incident Outcomes using the Probability column (denoted in blue) as the rate-parameter for the Monte Carlo Model. The dummy data dimension for the percentages of entity-level harm are then applied to the municipality dataset. For simplicity, these figures are in the aggregate. If the underlying population of individuals are made visible during the data collection phase, this analysis can be easily converted to include per capita, rather than aggregate figures.

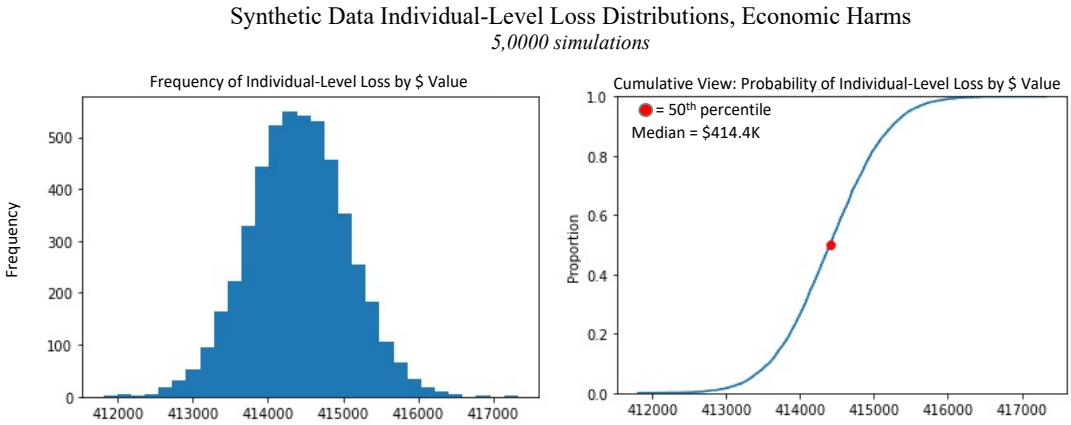

Figure 3: Synthetic data; Frequency and Cumulative views of Aggregated Individual Level Loss Distributions, Economic harms

Just as with the Bottoms-Up approach, a distribution of the probable size of aggregate harm to individuals can be calculated. Once the data is collected, this method provides a structured, repeatable individual harm estimation framework without the need of analyzing every incident in a dataset. The collection of the necessary data is a fundamental dependency. Value can be demonstrated incrementality if Incident Outcome data is collected iteratively, and then be applied on a per capita basis.

With value of estimating the magnitude of individual harms established, we now provide a brief discussion regarding potential means of compensating individuals for the cyber harms experienced.

Chapter 4: Mechanisms for Remedy and Redress for Individual Cyber Harms

The purpose of naming, categorizing and estimating the scope of harm to individuals caused by a cyber incident is to inform novel solutions for remedy or redress. The legal definition of remedy is, "The manner in which a right is enforced or satisfied by a court when some harm or injury, recognized by society as a wrongful act, is inflicted upon an individual." [96] Redress includes the concept of relief, or "a means of obtaining a remedy" [97]. A remedy should be viewed as more of a treatment or a correction, whereas redress as compensation to make up for something that went awry and needs to be restored. In this chapter, we will review novel solutions that could rectify the individual harms experienced. We explore legal, governmental, and industry mechanisms for relief from cyber harms. Though the prior chapters discuss the quantification of cyber harms, the solutions proposed do not all require such a granular degree of harm size specificity. Rather, the harm estimation exercise can often serve as more of a "t-shirt sizing" effort, where degrees of small, medium and large can suffice and inform the remedial harm reduction action.

The solutions proposed are influenced by two key factors – whether the party responsible for the harm is clearly known, and whether the size of the harm is well-understood. The suggested mechanisms for remedy or redress are organized below based on these factors:

	Responsible party known	Responsible party unknown/unclear
Harm size known	*Torts*	*Cybersecurity Superfund, Federal taxes rebates*
Harm size unknown/unclear	*Statutory claims, enhanced security services*	*Current state*

Table 17: Matrix of proposed mechanisms for individual cyber harm remedy or redress

4.1 Scenario 1: Harm Size and Responsible Party Known – Torts

Restatement of the Law, Torts 2d lays out the definitions and criteria for violations and remedies in the US related to intentional harms, negligence, strict liability, as well as other types of wrongful injuries [98]. Negligence, for example, is defined in the context of torts as, "conduct which falls below the standard established by law for the protection of others against unreasonable risk of harm. It does not include conduct recklessly disregardful of an interest of others." [98] Essentially, a tort claim is available in the legal arena if specific requirements are met. There must be a "failure to meet a duty", a known responsible party, and a resulting harm [99]. If the accused wrongdoer is deemed responsible for the harm, the victim will be compensated by the responsible party [98].

Where the naming and sizing of individual cyber harm becomes essential is the tort requirement to prove damages [70]. Through the outlined Bottoms-Up measurement approach, the specific individual harm related to a cyber incident can be quantified and used in court to meet the necessary criteria. This is best applied when there is negligence of some sort at the organizational level, such as consistently unpatched vulnerable systems or poor compliance with security standards. To run through a scenario, let's say a ransomware attack shut down a town's systems due to poor vulnerability management practices related to the

city's Windows servers. If the cyber insurance claims totaled $100,000 in a town of 5,000 residents, the per capita entity-level harm would be $20. Using the findings derived from the Per Capita Bottoms-Up measurement approach, a multiplier of 1.92 can be applied to the $20 loss per capita. If the attack details meets the criteria for a tort claim, each resident could be entitled to an additional $38.40 if the analysis is leveraged. In fact, this systematic sizing of harm to individuals using the historical relationship between entity and individual losses could *allow* residents to meet the proof of harm requirements for a tort claim in the first place.

However, tort claims for security and privacy have historically proven difficult [70][100]. The closest precedent for cybersecurity tort claims is in the case of *Capital One Consumer Data Security Breach Litigation*, where the United States District Court for the Eastern District of Virginia assumed "a tort duty to protect personally identifiable information by representing to customers that they carefully safeguard this information" [101]. As the eligibility for tort claims in a security context progress beyond the state-level and become more widely accepted, the Taxonomy and harm assessment approaches laid out could prove valuable.

4.2 Scenario 2: Harm Size Unknown/Unclear, Responsible Party Known

4.2.1 Statutory Claims

Based on the legal precedent for data breaches set in *Spokeo, Inc. vs. Robins* and *Ramirez vs. TransUnion*, the potential for cyber harm, like identity theft resulting from a data breach, does not meet the requirement to show proof of harm [99]. However, these data breach cases are held to standards required for tort claims, where evidence of damages are

mandatory, when in fact they should be viewed as eligible for statutory claims [70][102]. This legal avenue for remedy is available without needing to demonstrate a high level of specificity or precision for the harm estimated. Statutes that provide for statutory damages, theoretically, simply require proof that an injury occurred, but not to a highly specific degree [100]. For example, violations of the Anti-Cybersquatting Consumer Protection Act provide damages if a domain name is pirated, with compensation to the victims ranging from $100 to $10,000, as well as ten times the maximum if the piracy was done willfully [103]. This ranging of potential awarded damages based on a rubric provides an opportunity for a more generalized individual cyber harm sizing exercise. In light of this, Case Study-Based Correlated Measures may be a worthy candidate to fill this gap. If historical cyber incident data can show a consistent pattern of linkage between specific dimensions of data/asset ownership rights, irreplaceability, and permanence of impact, this can then inform the gradation of statutory damages awarded. In truth, much work is necessary to shift claims of individualized cyber harms from statutory damages to tort claims given the lack of relevant cybersecurity statutes on the books. That being said, the proposal outlined here could be beneficial to explore in parallel.

4.2.2 Enhanced Security Services

Stepping away from the strictly legal mechanisms for redress, enhanced security services to affected victims is another viable option when the responsible party is known but the exact size of the harm remains opaque. For example, as a byproduct of the Equifax Data Breach settlement, the Federal Trade Commission and Consumer Financial Protection Bureau mandated free membership to Experian IdentityWorks for four years to monitoring

potential identity theft for individuals with exposed personal information in the 2017 Equifax data breach [104]. While we do not endorse a solution that relies on a questionable service highly related to the responsible party, the general concept should not be ignored. It should not take a settlement to provide these services. Instead, the individual harm-sizing exercise can be conducted by enterprises or regulators to understand the nature and extent of the cyber harm. For example, if data is collected for Incident Outcomes related to compromised Electronic Medical Records at hospitals, either Bottoms-up or Case-Based methods can be applied. For Per Capita Bottoms-up Measures, if the harm to individuals exceeds an established threshold (an entity-level multiplier of .5 or greater per capita individual losses to patients, for example), then new monitoring services can automatically be provided to mitigate these additional negative impacts to patients. More robust security controls, like advanced threat monitoring on a home network, could be provided as well.

4.3 Scenario 3: Harm Size Known, Responsible Party Unknown/Unclear

We hypothesize that the area with the most potential to close the cyber harm gap via the Taxonomy for Individual Cyber Harms and the associated measurement methodologies are scenarios in which the responsible parties are unknown or unclear, but the general size of the harm is known. While there are a dearth of solutions in this category today, there is also the lowest likelihood for pushback. This is because a responsible party is not actively fighting the claims. Instead, the government is providing compensation for individual cyber harms through a novel set of solutions that build on existing remedies in similarly structured ecosystems that generate negative externalities.

4.3.1 Cybersecurity Superfund

For societal issues related to the environment and the health of a population, it is often difficult to stop the issue at the source or address individual claims of harm. This is because there are confounding factors that also could negatively impact a life. For instance, air pollution, a common negative externality example, is a result of standard business activities that, under unregulated market conditions, produce pollutants that harm the health of individuals [105]. However, stripping out whether other risk factors like smoking, rather than industry-produced air pollution, negatively impacted an individual can be difficult.

While there are numerous mechanisms that price-in the cost of negative externalities, we believe the concept of a superfund is ripe for application in a cybersecurity context. Superfund is the colloquial term used for the Comprehensive Environmental Response, Compensation and Liability Act (CERLA), created by Congress in the 1980s and overseen by the US Environmental Protection Agency [106]. The law created a tax on chemical and petroleum firms, and built up a trust fund of $1.6 billion dollars to clean up “abandoned or uncontrolled hazardous waste sites” [106]. Superfund comes with requirements and provides authority for different remedial actions to reduce hazardous waste in the name of safeguarding the health of individuals [107].

This concept can be leveraged to compensate individuals for harm experienced by cyber attacks targeted at entities via a Cybersecurity Superfund. As mentioned in our discussion on tort claims, proving a linkage between a quantifiable harm and a responsible party is difficult, and this results in barriers for much-needed redress. A creation of a Superfund for individual victims of cyber incidents could help sidestep this ongoing issue. While companies across all sectors are exploited, technology firms would serve as reasonable

candidates for a tax given their level of capital available and contribution to vulnerable environments. An analysis of the historical size of harms through the proposed methodology could help inform policy-makers on Cybersecurity Superfund monetary targets, as well as how the remedial funds should be allocated. For example, our Per Capita Bottoms-up analysis shows that attacks on police stations that do not shut down 9-1-1 include additional losses to residents, amounting to 73% of direct costs to the entity. Policy-makers can analyze the estimated frequency of future attacks on police stations and review the historical data on direct costs. The Cybersecurity Superfund can then set a monetary target aligned with 73% of those costs for the purposes of providing compensation or remediation services directly to affected residents in the future.

Note that while this proposal is tagged to the unknown or unclear responsible party category, the EPA's Superfund cleanup efforts are funded by potentially responsible parties (PRPs) about 70% of the time [108]. A similar division can be asserted for the Cybersecurity Superfund where legal claims fall short, providing incentives for targeted entities to uplift their security processes and capabilities to avoid future payout to the Superfund.

4.3.2 Federal Tax Rebates

Federal tax rebates are an additional mechanism for awarding compensation to affected victims when the relative size of the harm is known, but the responsible parties are not. Additional tax relief based on certain criteria due to an experienced hardship is not a new concept. Due to the COVID-19 pandemic, Recovery Rebate Credits were issued to eligible taxpayers based on the 2021 fiscal year, and the Child Tax Credit increased [109]. Moving expenses are quantified and considered tax deductible if set criteria is met and all

expenses are both “reasonable” and “necessary” [110]. Similarly, a set of questions can be asked as part of the tax filing process that determine both the eligibility and extent of harm experienced due to a cyber incident. Through this proposal, the amount of relief provided should be informed by the Taxonomy and applicable harm sizing methodology, as is detailed in the Superfund section above. The funds for the rebates would need to be approved and set aside by Congress, akin to the process followed for other tax rebates [109].

Chapter 5: Conclusion and Future Areas of Research

Through this body of research, we have demonstrated that harms to individuals as a result of institutions being exploited not only go uncaptured today, but also account for an additional ~70% of harms when compared to organizational-level losses. This amounts to an 42% of total harms. Ignoring costs to individuals from loss calculations does a disserve to residents, end-users and everyday consumers. Without the ability to identify and size individual cyber harms, there are few opportunities for meaningful recourse or redress. By combining our proposed Taxonomy and measurement approaches with legal, market-based, and government-run remedies, individuals can be appropriately compensated and protected in the long-run.

The subject of individual cyber harm categorization and measurement would benefit from several areas of additional research. First, we did not investigate in detail incentive structures that could prevent cyber attacks from successfully exploiting institutions in the first place. An interesting research question to explore would be, “What accountability models can be instituted to better align incentives amongst users and providers of goods and services that depend on technology?” This could include topics such as cyber insurance and liability, as well as product labeling (i.e., privacy and security “nutrition labels” [111]).

Substantial work is also still required to collect the necessary historical incident data for the alternative harm sizing method driven by Case Study-Based Correlated Measures. Without a firmer grasp on the relationship between entity-level and individual-level harms in the context of harm dimensions like ownership, irreplaceability, and permanence of impact, the framework lacks a more systematic, replicable approach.

A final area ripe for further analysis is a comparative review of individual cyber harm quantification for attacks that compromise data confidentiality versus data availability. The methods for estimating the impact for these two types of risks can be quite different, and drilling down a level further would be advantageous, improving the accuracy of harm sizing efforts.

There is still significant work to be done in the cyber risk, impact, and harm measurement space. We optimistically hope that our review of relevant literature, development of sizing methods and associated findings, and proposals for mechanisms to address individual cyber harm moves this area of research closer to the overall objective of providing protection for individuals who are casualties of broader technological and security challenges.

Bibliography

[1] "U.S. companies and cyber crime," *Statista*. http://www.statista.com/study/12881/smb-and-cyber-crime-in-the-united-states-statista-dossier/ (accessed Mar. 26, 2022).

[2] "Check Point Research: Cyber Attacks Increased 50% Year over Year," *Check Point Software*, Jan. 10, 2022. https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/ (accessed Apr. 04, 2022).

[3] "How a ransomware attack works - The Washington Post." https://www.washingtonpost.com/technology/2021/07/09/how-ransomware-attack-works/ (accessed Apr. 04, 2022).

[4] W. Banks, "Cyber Attribution and State Responsibility," *International Law Studies*, vol. 97, no. 1, Jul. 2021, [Online]. Available: https://digital-commons.usnwc.edu/ils/vol97/iss1/43

[5] "Analysis | Ransomware is wreaking havoc on U.S. cities," *Washington Post*. Accessed: Mar. 30, 2022. [Online]. Available: https://www.washingtonpost.com/politics/2021/09/07/cybersecurity-202-ransomware-is-wreaking-havoc-us-cities/

[6] Ponemon Institute Research Report, "The Economic Value of Prevention." https://info.deepinstinct.com/value-of-prevention (accessed Apr. 03, 2022).

[7] "Internet Crime Complaint Center(IC3) | Annual Reports." https://www.ic3.gov/Home/AnnualReports (accessed Mar. 26, 2022).

[8] I. Agrafiotis, J. R. C. Nurse, M. Goldsmith, S. Creese, and D. Upton, "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate," *Journal of Cybersecurity*, vol. 4, no. 1, p. tyy006, Jan. 2018, doi: 10.1093/cybsec/tyy006.

[9] "Cybersecurity Risks | NIST." https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/cybersecurity-risks (accessed Apr. 04, 2022).

[10] Z. Amin, "A practical road map for assessing cyber risk," *Journal of Risk Research*, vol. 22, no. 1, pp. 32–43, Jan. 2019, doi: 10.1080/13669877.2017.1351467.

[11] I. Aldasoro, L. Gambacorta, P. Giudici, and T. Leach, "The Drivers of Cyber Risk," Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 3613173, May 2020. Accessed: Mar. 30, 2022. [Online]. Available: https://papers.ssrn.com/abstract=3613173

[12] "Cybersecurity Risk Management: Frameworks, Plans, & Best Practices," *Hyperproof*, Sep. 08, 2021. https://hyperproof.io/resource/cybersecurity-risk-management-process/ (accessed Apr. 17, 2022).

[13] "Inside the plan to fix America's never-ending cybersecurity failures," *MIT Technology Review*. https://www.technologyreview.com/2022/03/18/1047395/inside-the-plan-to-fix-americas-never-ending-cybersecurity-failures/ (accessed Apr. 04, 2022).

[14] J. Mtsweni, N. Gcaza, and M. Thaba, "A unified cybersecurity framework for complex environments," in *Proceedings of the Annual Conference of the South*

African Institute of Computer Scientists and Information Technologists, New York, NY, USA, Sep. 2018, pp. 1–9. doi: 10.1145/3278681.3278682.
[15] A. Orlando, "Cyber Risk Quantification: Investigating the Role of Cyber Value at Risk," *Risks*, vol. 9, no. 10, Art. no. 10, Oct. 2021, doi: 10.3390/risks9100184.
[16] M. Bada and J. R. C. Nurse, "The Social and Psychological Impact of Cyber-Attacks," *arXiv:1909.13256 [cs]*, pp. 73–92, 2020, doi: 10.1016/B978-0-12-816203-3.00004-6.
[17] "What is Cyber Big Game Hunting? | CrowdStrike," *crowdstrike.com*. https://www.crowdstrike.com/cybersecurity-101/cyber-big-game-hunting/ (accessed Apr. 04, 2022).
[18] "The Unbalanced Negative Externalities of Cybersecurity," *The Security Ledger with Paul F. Roberts*, May 21, 2015. https://securityledger.com/2015/05/the-unbalanced-negative-externalities-of-cybersecurity/ (accessed Mar. 30, 2022).
[19] "CEA Report: The Cost of Malicious Cyber Activity to the U.S. Economy – The White House." https://trumpwhitehouse.archives.gov/articles/cea-report-cost-malicious-cyber-activity-u-s-economy/ (accessed Mar. 30, 2022).
[20] "What is the CIA Triad and Why is it important?," *Fortinet*. https://www.fortinet.com/resources/cyberglossary/cia-triad (accessed Apr. 17, 2022).
[21] "7 Cybersecurity Frameworks To Reduce Cyber Risk." https://www.bitsight.com/blog/7-cybersecurity-frameworks-to-reduce-cyber-risk (accessed Apr. 28, 2022).
[22] "Top 25 Cybersecurity Frameworks to Consider," *SecurityScorecard*. https://securityscorecard.com/blog/top-cybersecurity-frameworks-to-consider (accessed Apr. 28, 2022).
[23] "A Measurement Primer for Cybersecurity," in *How to Measure Anything in Cybersecurity Risk*, John Wiley & Sons, Ltd, 2016, pp. 19–34. doi: 10.1002/9781119162315.ch2.
[24] C. Whelan, "The 3 Problems with RCSA & How to Overcome Them with FAIR." https://www.fairinstitute.org/blog/the-3-problems-with-rcsa-how-to-overcome-them-with-fair (accessed Apr. 29, 2022).
[25] "Risk Matrices, Lie Factors, Misconceptions, and Other Obstacles to Measuring Risk," in *How to Measure Anything in Cybersecurity Risk*, John Wiley & Sons, Ltd, 2016, pp. 81–110. doi: 10.1002/9781119162315.ch5.
[26] B. Sheehan, F. Murphy, A. N. Kia, and R. Kiely, "A quantitative bow-tie cyber risk classification and assessment framework," *Journal of Risk Research*, vol. 24, no. 12, pp. 1619–1638, Dec. 2021, doi: 10.1080/13669877.2021.1900337.
[27] K. Ruan, "Introducing cybernomics: A unifying economic framework for measuring cyber risk," *Computers & Security*, vol. 65, pp. 77–89, Mar. 2017, doi: 10.1016/j.cose.2016.10.009.
[28] C. C. Editor, "security control - Glossary | CSRC." https://csrc.nist.gov/glossary/term/security_control (accessed Apr. 28, 2022).
[29] "The 18 CIS Controls," *CIS*. https://www.cisecurity.org/controls/cis-controls-list/ (accessed Aug. 27, 2021).

[30] “CIS Controls Self Assessment Tool (CIS CSAT),” *CIS*. https://www.cisecurity.org/controls/cis-controls-self-assessment-tool-cis-csat/ (accessed Apr. 28, 2022).
[31] “MITRE ATT&CK®.” https://attack.mitre.org/ (accessed Apr. 28, 2022).
[32] “HITRUST Alliance | HITRUST CSF | Information Risk Management,” *HITRUST Alliance*. https://hitrustalliance.net/product-tool/hitrust-csf/ (accessed Apr. 28, 2022).
[33] nicole.keller@nist.gov, “Cybersecurity Framework,” *NIST*, Nov. 12, 2013. https://www.nist.gov/cyberframework (accessed Aug. 27, 2021).
[34] swenson, “Cybersecurity Framework,” *NIST*, Mar. 13, 2017. https://www.nist.gov/industry-impacts/cybersecurity-framework (accessed Apr. 04, 2022).
[35] “Cybersecurity Frameworks 101 – The Complete Guide,” *The Missing Report*, Nov. 08, 2021. https://preyproject.com/blog/en/cybersecurity-frameworks-101/ (accessed Apr. 05, 2022).
[36] “What Is Personal Cyber Insurance? And How Can Homeowners Buy a Policy?,” *ValuePenguin*. https://www.valuepenguin.com/personal-cyber-home-insurance (accessed Mar. 30, 2022).
[37] S. Romanosky, L. Ablon, A. Kuehn, and T. Jones, “Content analysis of cyber insurance policies: how do carriers price cyber risk?,” *Journal of Cybersecurity*, vol. 5, no. 1, p. tyz002, Jan. 2019, doi: 10.1093/cybsec/tyz002.
[38] “People Don’t Care About Cybersecurity,” Mar. 07, 2019. https://modernciso.com/2019/03/07/people-dont-care-about-cybersecurity/ (accessed Apr. 29, 2022).
[39] K. Levy and B. Schneier, “Privacy Threats in Intimate Relationships,” Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 3620883, Jun. 2020. Accessed: Mar. 30, 2022. [Online]. Available: https://papers.ssrn.com/abstract=3620883
[40] nakia.grayson@nist.gov, “Risk Assessment Tools,” *NIST*, Oct. 28, 2018. https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/collaboration-space/focus-areas/risk-assessment/tools (accessed Apr. 28, 2022).
[41] https://www.eff.org, “Your Security Plan,” *Surveillance Self-Defense*, Aug. 01, 2014. https://ssd.eff.org/en/module/your-security-plan (accessed Mar. 30, 2022).
[42] https://www.eff.org, “Threat model,” *Surveillance Self-Defense*. https://ssd.eff.org/en/glossary/threat-model (accessed Apr. 29, 2022).
[43] “Protect Your Personal Information and Data,” *Consumer Advice*, May 26, 2021. http://consumer.ftc.gov/articles/protect-your-personal-information-data (accessed Apr. 29, 2022).
[44] C. C. Editor, “impact - Glossary | CSRC.” https://csrc.nist.gov/glossary/term/impact (accessed Apr. 29, 2022).
[45] “The Six Types of Loss in Cyber Incidents.” https://www.risklens.com/resource-center/blog/the-six-types-of-loss-in-cyber-incidents (accessed Apr. 04, 2022).
[46] OECD, “Encouraging Clarity in Cyber Insurance Coverage: Therole of public policy and regulation.” 2020. [Online]. Available: www.oecd.org/finance/insurance/Encouraging-Clarity-in-Cyber-Insurance-Coverage.pdf

[47] T. B. of C. Secretariat, “Guide to Risk Taxonomies,” Jun. 20, 2011. https://www.canada.ca/en/treasury-board-secretariat/corporate/risk-management/taxonomies.html (accessed Apr. 29, 2022).
[48] “Evaluation of Comprehensive Taxonomies for Information Technology Threats,” *CSIAC*. https://csiac.org/articles/evaluation-of-comprehensive-taxonomies-for-information-technology-threats/ (accessed Apr. 29, 2022).
[49] “Model Now!,” in *How to Measure Anything in Cybersecurity Risk*, John Wiley & Sons, Ltd, 2016, pp. 35–54. doi: 10.1002/9781119162315.ch3.
[50] “Cyber Security Risk Modeling: What Is It And How Does It Benefit You.” https://www.bitsight.com/blog/cyber-security-risk-modeling (accessed Apr. 29, 2022).
[51] F. Institute, “The Importance and Effectiveness of Cyber Risk Quantification.” https://www.fairinstitute.org/what-is-fair (accessed Mar. 31, 2022).
[52] T. M. and D. Musselwhite, “Primary vs. Secondary Loss in FAIR™ Analysis: What’s the Difference and Why It Matters.” https://www.fairinstitute.org/blog/primary-vs.-secondary-loss-in-fair-analysis-whats-the-difference-and-why-it-matters (accessed Apr. 29, 2022).
[53] “CyberVaR: Quantifying the risk of loss from cyber attacks | Premiere Speakers Bureau,” *premierespeakers.com*. https://premierespeakers.com//rod_beckstrom/blog/2014/12/16/cybervar_quantifying_the_risk_of_loss_from_cyber_attacks (accessed Apr. 29, 2022).
[54] A. Erola, I. Agrafiotis, J. R. C. Nurse, L. Axon, M. Goldsmith, and S. Creese, “A system to calculate Cyber Value-at-Risk,” *Computers & Security*, vol. 113, p. 102545, Feb. 2022, doi: 10.1016/j.cose.2021.102545.
[55] “What is Cyber Risk? Definition & Examples,” *SecurityScorecard*. https://securityscorecard.com/blog/what-is-cyber-risk-definition-examples (accessed Apr. 04, 2022).
[56] “Why Cybersecurity Rating Matters In The Era Of Growing Digital Transformation,” *Toolbox*. https://www.toolbox.com/it-security/cyber-risk-management/articles/why-cybersecurity-ratings-matters/ (accessed Apr. 29, 2022).
[57] “A Framework for Predicting Data Breach Risk: Leveraging Dependence to Cope With Sparsity | IEEE Journals & Magazine | IEEE Xplore.” https://ieeexplore-ieee-org.libproxy.mit.edu/document/9323027 (accessed Apr. 29, 2022).
[58] “Reputational damage and cyber risk go hand in hand | Aon.” https://www.aon.com/unitedkingdom/insights/reputational-damage-and-cyber-risk.jsp (accessed Aug. 27, 2021).
[59] “2021 DBIR Results & Analysis,” *Verizon Business*. https://www.verizon.com/business/resources/reports/dbir/2021/results-and-analysis/ (accessed Apr. 01, 2022).
[60] “Cost of a Data Breach Report 2021,” Sep. 08, 2021. https://www.ibm.com/security/data-breach (accessed Apr. 29, 2022).
[61] “SCRAM: A Platform for Securely Measuring Cyber Risk · Issue 2.3, Summer 2020.” https://hdsr.mitpress.mit.edu/pub/gylaxji4/release/4 (accessed Apr. 04, 2022).
[62] “MIT SCRAM – Secure Cyber Risk Aggregation and Measurement.” https://scram.mit.edu/ (accessed Aug. 27, 2021).

[63] “The Hidden Costs of Cybercrime.” https://www.csis.org/analysis/hidden-costs-cybercrime (accessed Mar. 30, 2022).
[64] “Seven Hidden Costs of a Cyberattack,” *Deloitte United States*. https://www2.deloitte.com/us/en/pages/finance/articles/cfo-insights-seven-hidden-costs-cyberattack.html (accessed Apr. 29, 2022).
[65] “Standing in Data-Breach Actions: Injury in Fact?,” *Lawfare*, Dec. 18, 2017. https://www.lawfareblog.com/standing-data-breach-actions-injury-fact (accessed Apr. 29, 2022).
[66] “Definition of HARM.” https://www.merriam-webster.com/dictionary/harm (accessed Apr. 29, 2022).
[67] “injury,” *LII / Legal Information Institute*. https://www.law.cornell.edu/wex/injury (accessed Apr. 30, 2022).
[68] I. Agrafiotis *et al.*, “Cyber Harm: Concepts, Taxonomy and Measurement,” Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 2828646, Aug. 2016. doi: 10.2139/ssrn.2828646.
[69] Federal Bureau of Investigation, “Internet Crime Complaint Center (IC3) | Internet Crime Report 2021.” 2021.
[70] D. K. Citron and D. J. Solove, “Privacy Harms,” Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 3782222, Feb. 2021. doi: 10.2139/ssrn.3782222.
[71] “Privacy Harms: A Taxonomy to Understand Privacy Violations,” *THE EXTENDED MIND*. https://www.extendedmind.io/the-extended-mind-blog/2021/04/06/2021-4-6-privacy-harms-a-taxonomy-to-understand-privacy-violations (accessed Apr. 02, 2022).
[72] *Measuring and Managing Information Risk*. Accessed: Apr. 30, 2022. [Online]. Available: https://learning.oreilly.com/library/view/measuring-and-managing/9780124202313/
[73] “What is NotPetya? 5 Fast Facts | Security Encyclopedia,” *HYPR*. https://www.hypr.com/notpetya/ (accessed Apr. 30, 2022).
[74] A. Greenberg, “The Untold Story of NotPetya, the Most Devastating Cyberattack in History,” *Wired*. Accessed: Mar. 30, 2022. [Online]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
[75] E. Stewart, “Hackers have been holding the city of Baltimore’s computers hostage for 2 weeks,” *Vox*, May 21, 2019. https://www.vox.com/recode/2019/5/21/18634505/baltimore-ransom-robbinhood-mayor-jack-young-hackers (accessed Feb. 11, 2021).
[76] “6 cases where the Ashley Madison leak has ensnared political and public officials - The Washington Post.” https://webcache.googleusercontent.com/search?q=cache:mdMpZhDMcdgJ:https://www.washingtonpost.com/news/the-fix/wp/2015/08/26/6-cases-where-the-ashley-madison-leak-has-ensnared-political-and-public-officials/+&cd=6&hl=en&ct=clnk&gl=us (accessed May 01, 2022).

[77] E. Dallaway, "Victims of cybercrime are suffering emotional trauma," *Infosecurity Magazine*, Sep. 12, 2016. https://www.infosecurity-magazine.com/news/isc2congress-cybercrime-victims/ (accessed Apr. 03, 2022).
[78] "Should the Law Recognize 'Privacy Harms'?," *American Enterprise Institute - AEI*, Feb. 19, 2021. https://www.aei.org/technology-and-innovation/should-the-law-recognize-privacy-harms/ (accessed May 01, 2022).
[79] "The Story of the Social Security Number," *Social Security Administration Research, Statistics, and Policy Analysis*. https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html (accessed May 01, 2022).
[80] "Ask the Expert: What Does the Constitution Say About Education? Nothing Explicitly, But That Doesn't Mean it Can't Help Provide Students with Equal Educational Access, Says Assistant Professor Jenn Ayscue," *College of Education News*. https://ced.ncsu.edu/news/2020/09/18/ask-the-expert-what-does-the-constitution-say-about-education-nothing-explicitly-but-that-doesnt-mean-it-cant-help-provide-students-with-equal-educational-access-says-assistant-p/ (accessed May 01, 2022).
[81] "How to protect yourself against the theft of your identity | The Economist." https://webcache.googleusercontent.com/search?q=cache:xn0_L1D-UYIJ:https://www.economist.com/finance-and-economics/2017/09/14/how-to-protect-yourself-against-the-theft-of-your-identity+&cd=1&hl=en&ct=clnk&gl=us (accessed Apr. 25, 2022).
[82] M. Honan, "Mat Honan: How I Resurrected My Digital Life After an Epic Hacking," *Wired*. Accessed: Apr. 03, 2022. [Online]. Available: https://www.wired.com/2012/08/mat-honan-data-recovery/
[83] M. Honan, "How Apple and Amazon Security Flaws Led to My Epic Hacking," *Wired*. Accessed: Apr. 03, 2022. [Online]. Available: https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/
[84] "What is lateral movement in cyber security?," *Cloudflare*. https://www.cloudflare.com/learning/security/glossary/what-is-lateral-movement/ (accessed May 01, 2022).
[85] D. Temple-Raston, "A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack," *NPR*, Apr. 16, 2021. Accessed: May 01, 2022. [Online]. Available: https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack
[86] "Password reuse, credential stuffing and another billion records in Have I been pwned," *Troy Hunt*, May 04, 2017. https://www.troyhunt.com/password-reuse-credential-stuffing-and-another-1-billion-records-in-have-i-been-pwned/ (accessed May 01, 2022).
[87] "What Is a Monte Carlo Simulation?," *Investopedia*. https://www.investopedia.com/terms/m/montecarlosimulation.asp (accessed Apr. 27, 2022).
[88] "Poisson Distribution | Brilliant Math & Science Wiki." https://brilliant.org/wiki/poisson-distribution/ (accessed Apr. 28, 2022).

[89] W. Koehrsen, "The Poisson Distribution and Poisson Process Explained," *Medium*, Aug. 20, 2019. https://towardsdatascience.com/the-poisson-distribution-and-poisson-process-explained-4e2cb17d459 (accessed Apr. 28, 2022).
[90] S. Gonzalez, "How Government Agencies Determine The Dollar Value Of Human Life," *NPR*, Apr. 23, 2020. Accessed: Apr. 26, 2022. [Online]. Available: https://www.npr.org/2020/04/23/843310123/how-government-agencies-determine-the-dollar-value-of-human-life
[91] "Measuring the Risk in High–Low Frequency Tasks." https://www.securitymagazine.com/blogs/14-security-blog/post/83398-measuring-the-risk-in-high-low-frequency-tasks (accessed Apr. 27, 2022).
[92] "Why Do Cyber Liability Claims Cost So Much? | Insureon." https://www.insureon.com/blog/why-do-cyber-liability-claims-cost-so-much (accessed May 01, 2022).
[93] "Average length of downtime after a ransomware attack 2021," *Statista*. http://www.statista.com/statistics/1275029/length-of-downtime-after-ransomware-attack/ (accessed May 01, 2022).
[94] "Critical Infrastructure Sectors | CISA." https://www.cisa.gov/critical-infrastructure-sectors (accessed Feb. 11, 2021).
[95] "Baltimore City Ransomware Attack Knocks City Services Offline : NPR." https://www.npr.org/2019/05/21/725118702/ransomware-cyberattacks-on-baltimore-put-city-services-offline (accessed Feb. 11, 2021).
[96] "Remedy," *The Free Dictionary*. Accessed: May 02, 2022. [Online]. Available: https://legal-dictionary.thefreedictionary.com/Remedy
[97] "Definition of REDRESS." https://www.merriam-webster.com/dictionary/redress (accessed May 02, 2022).
[98] *Restatement of the Law, Second, Torts 2d*. St. Paul, MN: American Law Institute Publishers, 1965. Accessed: May 12, 2022. [Online]. Available: https://advance-lexis-com.libproxy.mit.edu/
[99] W. Gamble, "How The Tort of Negligence Affects Data Breach Lawsuits," *IT Governance USA Blog*, Feb. 24, 2022. https://www.itgovernanceusa.com/blog/how-the-tort-of-negligence-affects-data-breach-lawsuits (accessed Apr. 16, 2022).
[100] D. Chase, "Cybersecurity Law and Theories of Harm: The Lay of the Land," *Medium*, Apr. 05, 2018. https://medium.com/@Daniel_Chase_/cybersecurity-law-and-theories-of-harm-the-lay-of-the-land-e95a92cde9fb (accessed Apr. 17, 2022).
[101] "Questions About Tort and Contract Claims in the Cybersecurity Context Left Unsettled," *Woods Rogers PLC*, Nov. 30, 2021. https://www.woodsrogers.com/questions-about-tort-and-contract-claims-in-the-cybersecurity-context-left-unsettled/ (accessed May 02, 2022).
[102] "Facts Matter—TransUnion's Impact on Privacy, Cybersecurity Litigation." https://news.bloomberglaw.com/us-law-week/facts-matter-transunions-impact-on-privacy-cybersecurity-litigation (accessed Apr. 17, 2022).
[103] "Statutory Damages | UpCounsel 2022," *UpCounsel*. https://www.upcounsel.com/statutory-damages (accessed May 02, 2022).

[104] "Equifax Data Breach Settlement," *Federal Trade Commission*, Jul. 11, 2019. http://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement (accessed May 02, 2022).
[105] "The economics of pollution (article)," *Khan Academy*. https://www.khanacademy.org/economics-finance-domain/microeconomics/market-failure-and-the-role-of-government/environmental-regulation/a/the-economics-of-pollution-cnx (accessed Mar. 27, 2022).
[106] O. US EPA, "What is Superfund?," Nov. 09, 2017. https://www.epa.gov/superfund/what-superfund (accessed May 02, 2022).
[107] "What is Superfund | Superfund Research Program." https://deohs.washington.edu/srp/what-superfund (accessed May 02, 2022).
[108] U. L. Inc, "Comprehensive Environmental Response, Compensation, and Liability Act (CERLA or Superfund) – Environmental Law." https://environmentallaw.uslegal.com/federal-laws/comprehensive-environmental-response-compensation-and-liability-act-cerla-or-superfund/ (accessed May 02, 2022).
[109] "Guide to filing your taxes in 2022," *Consumer Financial Protection Bureau*. https://www.consumerfinance.gov/coronavirus/managing-your-finances/guide-filing-taxes-2022/ (accessed May 02, 2022).
[110] T.-T. Tax Income, "IRS Form 3903: Are Moving Expenses Tax Deductible?" https://turbotax.intuit.com/tax-tips/jobs-and-career/guide-to-irs-form-3903-moving-expenses/L6CwmGm3K (accessed May 02, 2022).
[111] "IoT labels will help consumers figure out which devices are spying on them." https://www.cylab.cmu.edu/news/2020/05/27-iot-labels-consumers.html (accessed Jul. 28, 2021).

Appendix A: Per Capita Bottoms-Up Measures

Appendix A1: Detailed View of Equations

Safety and Security Harms: Police Station

		Frequency of Event	Actualized Harm Factor (Amount of asset affected)	Potential Harm (Value of asset)	Calculation for Individual Cyber Harm
	Incident Outcome	f_i	π_i	v_i	*Moderate Scenario*
1	Police Station – 911 system down	240M calls per year in the US, per 332 million people = ~ .72 calls per person per year . 00198 calls to the police per person in municipality population per day *d*	Assumptions: - Required assistance cannot be provided to aid in prevention of loss of life - 6.4% of calls are violent crimes, with 1.4% of those being murder and nonnegligent manslaughter - 1% of calls are while a crime is in progress, and therefore can be prevented .000896 actualized harm factor applied in a moderate scenario, based on annual rates of violent crimes prevented while in progress	10 million, based on the Value of a Statistical Life (VoSL)	$= (.\mathbf{00198}\,\boldsymbol{d}) * (.\mathbf{000896} * \$\mathbf{10M})$
2	Police Station – All technology down, ex. 911	Number of incidents, multiplied by the # of days *d* over 365 days in a year	Assumption: Drop experienced in police productivity during attack *Moderate scenario:* 15% drop in productivity	Budget *b* is spent annually per capita on average on police force in a given US state = *b *population*	$= \left(\frac{\boldsymbol{d}}{\mathbf{365}}\right) * (.\mathbf{15} * \boldsymbol{b})$

References

Safety and Security Incident Outcome 1: [1] [2] [3] [4] [5] [6, p. 1] [7] [8] [9]

Safety and Security Incident Outcome 2: [2] [8]

Safety and Security Harms: Fire Department

		Frequency of Event	Actualized Harm Factor (Amount of asset affected)	Potential Harm (Value of asset)	Calculation for Individual Cyber Harm
	Incident Outcome	f_i	π_i	v_i	*Moderate Scenario*
3	Fire Department – Fire-related death	3704 deaths per year per 332M people = .0000112, broken down by day $3*10^{-8}$ deaths per person per day d	Assumptions: Across all scenarios, death occurred so no additional weighting is applied *Moderate scenario:* 1	10 million, based on the Value of a Statistical Life (VoSL)	$= (3*10^{-8}\boldsymbol{d}) * \mathbf{107}$
4	Fire Department – Fire-related injury	16,600 injuries per year per 332 million people = .00005, broken down by day $1.4*10^{-7}$ injuries per person per day d	Assumptions: Injuries of varying degrees inform a discounting of the VoSL figure *Moderate scenario:* 20%	10 million, based on the Value of a Statistical Life (VoSL)	$= (1.4*10^{-7}\boldsymbol{d}) * (.2 * \mathbf{107})$
5	Fire Department – EMS + Hazardous Conditions	27M calls per year in the US, per 332M people = .08133 .00022 calls per person per day d	Assumptions: - Required assistance cannot be provided to aid in prevention of loss of life - 64% of calls for EMS and 3.5% for hazardous conditions - 42% are for residential buildings - 20% fire department needed *Moderate scenario:* .0537 actualized harm factor applied in a moderate scenario	10 million, based on the Value of a Statistical Life (VoSL)	$= (.00022\boldsymbol{d}) * (5.38 \text{ x } 10{-}6 * 10^{7})$
6	Fire Department – All technology down	Number of incidents, multiplied by the # of days d over 365 days in a year	Assumption: Drop experienced in fire department productivity during attack *Moderate scenario:* 15% drop in productivity	Budget b is spent annually per capita on average on fire departments $= b$ **population*	$= \left(\frac{\boldsymbol{d}}{\mathbf{365}}\right) * (.15 * \boldsymbol{b})$

References

Safety and Security Incident Outcome 3: [1] [7] [10] [11]
Safety and Security Incident Outcome 4: [1] [7] [10] [11]
Safety and Security Incident Outcome 5: [1] [7] [10] [11] [12] [13]
Safety and Security Incident Outcome 6: [14] [15]

Safety and Security Harms: Sewage Pump Station

		Frequency of Event	Actualized Harm Factor (Amount of asset affected)	Potential Harm (Value of asset)	Calculation for Individual Cyber Harm
	Incident Outcome	f_i	π_i	v_i	*Moderate Scenario*
7	Sewage pumps station damage	Number of incidents = 1	Assumption: Degree of damage of sewage pump station may vary *Moderate scenario:* 50% damaged	Assumptions: - Although only a portion of a municipality's town is served by a sewage pump, the analysis spreads the risk across the entire population - Number of sewage pump stations affected *pump* - Full sewage pump improvement = ~ $20K $20,000 per *sewage station pump*	$= \frac{.5\ (20,000\ * \#\ of\ pumps)}{population}$

References

Safety and Security Incident Outcome 7: [16]

Economic Harms

		Frequency of Event	Actualized Harm Factor (Amount of asset affected)	Potential Harm (Value of asset)	Calculation for Individual Cyber Harm
	Incident Outcome	f_i	π_i	v_i	*Moderate Scenario*
1	Ransomware Attack shutdown systems	Assumption: Where no time interval was specified, the 2021 average of 22 days is used. 1 incident * (# of days *d* of a ransomware attack/365 days)	Assumption: Drop experienced in productivity of municipality services during attack *Moderate scenario:* 15% drop in productivity	Median annual property tax paid in state attack occurred, *t* Average number of people per household = 2.6 = *t* * (*population*/2.6)	$= \left(\frac{d}{365}\right) * \left(\frac{.15t}{2.6}\right)$
2	General breach of municipality network	Assumptions: - Where no time interval was specified, the 2019 average time from discovery to attack containment, 3 days, is used - Each day *d* represents 8 hours of working time 1 incident * 8 hours * (# of days *d* to contain an attack)	Assumptions: - Attack is resolved by municipality employees working in IT, called Full Time Equivalents, or FTE - For every 10K of a municipality population, another employee is required FTE = (*population*/10,000) *Moderate scenario:* Assumed number of employees needed	Average hourly IT municipality employee salary *s*, based on the state the attack occurs in = *s*	$= 8d * \left(\frac{1}{10{,}000}\right) * s$
3	Financial administration shut down	Assumptions: - Where no time interval was specified, the 2019 average time from discovery to attack containment, 3 days, is used 1 incident * (# of days *d* / 365 days in a year)	Assumption: Drop experienced in productivity during attack *Moderate scenario:* 15% drop in productivity	Use amount spent annually per capita in the state of that claim on finance administration, *spend* per municipality population = *spend* **population*	$= \left(\frac{d}{365}\right) * (.15 * spend)$

References

Economic Harm Incident Outcome 1: [1] [9] [17]
Economic Harm Incident Outcome 2: [14] [18]
Economic Harm Incident Outcome 3: [14] [15]

Economic Harms (continued)

		Frequency of Event	Actualized Harm Factor (Amount of asset affected)	Potential Harm (Value of asset)	Calculation for Individual Cyber Harm
	Incident Outcome	f_i	π_i	v_i	*Moderate Scenario*
4	Data breach, exposed PII	.00139 chance identity theft due to breach per person	Assumption: Discounting for likelihood that identity theft is caused directly by this breach or a previous breach *Moderate scenario:* 10% drop in productivity	On average, it takes 100 - 200 hours for an individual to recover from identity theft, so using a midpoint 150 hours Median hourly earnings in the US is $16.36 Median dollar value lost = $800	$= (1.39 * 10^{-3}) * (.1 * (150 * 16.36) + 800)$
5	Unrecovered stolen funds	Number of incidents = 1 incident	Assumption: The amount of unrecovered funds is set and does not align with conservative/moderate/aggressive scenarios	The analysis spreads the risk across the entire population *pop* = Stolen funds *stolen* - recovered funds *recovered*	$= \frac{stolen - recovered}{pop}$
6	Municipality employee identity theft	Number of incidents = 1 incident	Assumption: - The attack on municipal employees reduces productivity to serve the municipality - Discounts the number of hours worked to recover from identity theft *Moderate:* Assumed number of employee hours required	Average hourly IT municipality employee salary *s*, based on the state the attack occurs in Number of employees affected, *e* On average, it takes 100 - 200 hours for an individual to recover from identity theft, so using a midpoint 150 hours = 150 * *s* * *e*	$= \frac{150 * s * e}{pop}$
7	Endpoint data destruction, requiring recovery	Number of incidents = 1 incident	Assumption: Degree of damage of hard drive may vary *Moderate scenario:* Average Potential Harm	Assumptions - Average data recovery cost per asset *asset* is about $1,000 = 1000 * *asset*	$= \frac{1,000 * asset}{pop}$
Note: Calculations for 5-7 do not scale by population. The risk is still spread across a municipality's population, but does not cancel out with any figure in the numerator and therefore remains in the final equations in the last column.					

References

Economic Harm Incident Outcome 4: [19] [20]
Economic Harm Incident Outcome 5: None, derived from claims data only
Economic Harm Incident Outcome 6: [18] [21]
Economic Harm Incident Outcome 7: [22]

Reputational Harms

		Frequency of Event	Actualized Harm Factor (Amount of asset affected)	Potential Harm (Value of asset)	Calculation for Individual Cyber Harm
	Incident Outcome	f_i	π_i	v_i	*Moderate Scenario*
1	Sensitive information exposed regarding criminal behavior	10 million arrests in the US per year out of a population of 332 million (ignoring repeat offenders for this analysis) = 8.25 * 10^{-5} arrests per person per day *d* of exposed police log data = 8.25 * 10^{-5} * *population* * $(\frac{d}{365})$	Assumption: Degree of harm experienced by known sensitive information *Moderate scenario:* 2% affected	Assumption: - Missed job opportunities - 2021 median annualized salary of $34,600 - 7 years before expunging record = 34,600 * 7 per *population*	$= \left(8.25*10^{-5} * \frac{d}{365}\right) * .2 * 242,200$

References

Reputational Harm Incident Outcome 1: [23] [24]

Psychological Harms

		Frequency of Event	Actualized Harm Factor (Amount of asset affected)	Potential Harm (Value of asset)	Calculation for Individual Cyber Harm
	Incident Outcome	f_i	π_i	v_i	*Moderate Scenario*
1	Impact to children's access to education	Assumptions: Where no time interval was specified, the 2019 average time from discovery to attack containment, 3 days, is used 1 incident * (days *d* to contain an attack/365 days)	Assumption: Degree of student education affected may vary *Moderate scenario:* 50% affected	Number of schools affected *school* Assumptions: - $14.5K spent per student annually by taxpayers - 500 students per school = 14,500 * (500 * *school)*	$= \frac{\frac{d}{365} * .5\ (14,500\ * 500 * school)}{pop}$

References

Psychological Harm Incident Outcome 1: [1] [14] [25] [26]

Appendix A2: Per Capita Bottoms-Up Measures – References

[1] "U.S. Census Bureau QuickFacts: United States." https://www.census.gov/quickfacts/fact/table/US/HCN010212 (accessed May 11, 2022).
[2] "Solutions & Research," *Vera Institute of Justice*. https://www.vera.org/solutions-research (accessed May 11, 2022).
[3] "Criminal Justice Researchers Studied Over 4 Million 911 Calls. Here's How Their Findings Could Influence Calls for Police Reform," *Time*. https://time.com/6090633/911-calls-criminal-justice-study-defund-police/ (accessed Apr. 26, 2022).
[4] "Changing Police Practices Means Changing 911," *Vera Institute of Justice*. https://www.vera.org/news/changing-police-practices-means-changing-911 (accessed May 11, 2022).
[5] "Violent Crime," *FBI*. https://ucr.fbi.gov/crime-in-the-u.s/2019/crime-in-the-u.s.-2019/topic-pages/violent-crime (accessed May 11, 2022).
[6] "Table 1," *FBI*. https://ucr.fbi.gov/crime-in-the-u.s/2019/crime-in-the-u.s.-2019/tables/table-1/table-1.xls (accessed May 11, 2022).
[7] S. Gonzalez, "How Government Agencies Determine The Dollar Value Of Human Life," *NPR*, Apr. 23, 2020. Accessed: Apr. 26, 2022. [Online]. Available: https://www.npr.org/2020/04/23/843310123/how-government-agencies-determine-the-dollar-value-of-human-life
[8] "The States That Spend the Most on Policing and Corrections | MoneyGeek.com." https://www.moneygeek.com/living/state-policing-corrections-spending/ (accessed May 11, 2022).
[9] "Average length of downtime after a ransomware attack 2021," *Statista*. http://www.statista.com/statistics/1275029/length-of-downtime-after-ransomware-attack/ (accessed May 01, 2022).
[10] "Fire Department Overall Run Profile (2019)," *U.S. Fire Administration*, Apr. 21, 2021. https://www.usfa.fema.gov/data/statistics/reports/run_profile_v21i1.html (accessed May 11, 2022).
[11] "U.S. fire statistics," *U.S. Fire Administration*, Mar. 25, 2022. https://www.usfa.fema.gov/data/statistics/index.html (accessed May 11, 2022).
[12] B. McSheffrey, "Fire Extinguishers Extinguish an Estimated 5.32 Million Fires in US in 2010." http://www.engaugeinc.net/life-and-fire-safety-blog/fire-extinguishers-extinguish-an-estimated-532-million-fires-in-us-in-2010 (accessed May 11, 2022).
[13] "2022 ESO Fire Service Index," *ESO*. https://www.eso.com/resources/fire-index/ (accessed May 11, 2022).
[14] "U.S. cyber incident response lifecycle 2019," *Statista*. http://www.statista.com/statistics/194119/average-time-span-until-a-cybercrime-incident-is-resolved/ (accessed Apr. 26, 2022).
[15] Municipality Budget - Source masked to maintain privacy of dataset
[16] Municipality Budget - Source masked to maintain privacy of dataset

[17] State Property Taxes - Source masked to maintain privacy of dataset
[18] “Job Search - Millions of Jobs Hiring Near You,” *ZipRecruiter*, specific job salary masked to maintain privacy of dataset
[19] “50+ Identity Theft & Credit Card Fraud Statistics (2022),” *Define Financial*, Jan. 10, 2022. https://www.definefinancial.com/blog/identity-theft-credit-card-fraud-statistics/ (accessed Apr. 26, 2022).
[20] “Wage and salary workers in the U.S.: hourly earnings 1979-2020,” *Statista*. http://www.statista.com/statistics/185335/median-hourly-earnings-of-wage-and-salary-workers/ (accessed May 11, 2022).
[21] “How to protect yourself against the theft of your identity | The Economist.” https://webcache.googleusercontent.com/search?q=cache:xn0_L1D-UYIJ:https://www.economist.com/finance-and-economics/2017/09/14/how-to-protect-yourself-against-the-theft-of-your-identity+&cd=1&hl=en&ct=clnk&gl=us (accessed Apr. 25, 2022).
[22] “What Does Data Recovery Cost? A Breakdown of Rates & Fees,” Jun. 29, 2020. https://www.provendatarecovery.com/blog/data-recovery-cost-rates-fees/ (accessed Apr. 25, 2022).
[23] SueKunkel, “Average wages, median wages, and wage dispersion.” https://www.ssa.gov/oact/cola/central.html (accessed May 11, 2022).
[24] R. R. Foundation, “Total Annual Arrests in the US by Type of Offense,” *Drug Policy Facts*, Jul. 07, 2021. https://www.drugpolicyfacts.org/node/235 (accessed Apr. 26, 2022).
[25] M. Riser-Kositsky, “Education Statistics: Facts About American Schools,” *Education Week*, Jan. 03, 2019. Accessed: May 11, 2022. [Online]. Available: https://www.edweek.org/leadership/education-statistics-facts-about-american-schools/2019/01
[26] “U.S. Public Education Spending Statistics [2022]: per Pupil + Total,” *Education Data Initiative*. https://educationdata.org/public-education-spending-statistics (accessed Apr. 26, 2022).

Appendix B: Implementation of Simulations

```
import pandas as pd
import numpy as np
import matplotlib.pyplot as plt
import random
import seaborn as sns


### Functions ###

def Lambda_create (cat_array, time_annual):
    """
    Input: Loss should still be in array form
    Find rates of loss
    Output: Singular row of rates and losses per simulation

    """

    if type(cat_array) == list:
        attack_rate = 1 / time_annual
        sum_array = cat_array

    else:
        attack_rate = (len(cat_array)) / time_annual
        #print("Attack rate: ", attack_rate)

        sum_array = np.sum(cat_array, axis=0)
        #print("Array of summed losses: ", sum_array)

    loss_rates = np.true_divide(sum_array, time_annual)
    #print("Loss_rates array:", loss_rates)

    # This should be annual rates for the following:
    # Attack frequency, Entity-level loss, individual-losses

    freq_array = np.insert(loss_rates, 0, attack_rate)
    #print ("freq array:", freq_array)

    return freq_array


def plot_MonteCarlo (econ_rates, ss_rates, rep_rates, psych_rates,
```

```
                    agg_rates, iters):
    """
    Input: Lambdas for each category array, # of simulations
    Complete simulation
    Output: Distributions for each Harm Type within the Taxonomy

    Legend for Harm Type:
        Harm Type 1: Economic Harm
        Harm Type 2: Safety & Security Harm
        Harm Type 3: Reputational Harm
        Harm Type 4: Psychological Harm
        Harm Type 5: Aggregated View across all harm types
    """

    lambdas_array = econ_rates
    lambdas_array = np.vstack((lambdas_array, ss_rates, rep_rates,
                               psych_rates, agg_rates))
    #print("lambdas array: ", lambdas_array)
    rows, cols = lambdas_array.shape

    i = 0
    while i < cols:
        for j in range (rows):
            simulated_data = np.random.poisson(lambdas_array[j][i],
iters)
            #print("simulated data: ", simulated_data)

           ### Plotting Distributions ###
            plt.hist (simulated_data, bins=30)
            median_val = np.percentile(simulated_data, 50)
            if i == 0:
                plt.title('Attack Frequency, Harm Type '+str(j+1)+'')
                #print('Median value for Attack Frequency, Harm Type:
                    #'+str(j+1)+'' , median_val)
                #print ('Mean: ', np.mean(simulated_data))
            elif i == 1:
                plt.title('City-level Loss, Harm Type: '+str(j+1)+'')
                #print('Median value for City-level Loss, Harm Type:
                    #'+str(j+1)+'' , median_val)
                #print ('Mean: ', np.mean(simulated_data))
            elif i == 2:
                plt.title('Individual Loss Option 1, Harm Type:
'+str(j+1)+'')
                #print('Median value for Individual Loss 01, Harm
Type:
                    #'+str(j+1)+'' , median_val)
                #print ('Mean: ', np.mean(simulated_data))
            elif i == 3:
                plt.title ('Individual Loss Option 2, Harm Type:
```

```
'+str(j+1)+'')
                #print('Median value for Individual Loss 02, Harm
Type:
                    #'+str(j+1)+'' , median_val)
                #print ('Mean: ', np.mean(simulated_data))

            else:
                break

            plt.show()

            ### Plotting Cumulative View ###
            sns.ecdfplot(simulated_data)
            plt.title('Cumulative Version')
            plt.plot(median_val, .5, marker ='o', color = 'red',
                     linestyle='none')
            plt.show()

        i += 1

### Dummy Attack Profiles ###
## Delete once data is collected via future research effort
regime_distros_econ = np.array([["credit card", 25, 2,0,.5,5],
                      ["social security number", 75, 7, 5, 2, 10]])

def calc_IL2 (harm_array, regime_distros):

    '''
    Input:  Array of entity-level losses and bottoms-up losses (if
calculated)
    by Harm Type, with empty last column
            Regime_distros are the Attack Profiles, organized as
follows:
                Each row reprsents an Attack Profile
                Column 1: Attack Profile Name (e.g., credit card
theft)
                Column 2: Share (e.g., frequency) of the attack
profile for all
                          claims associated with that Harm Type
                Column 3: Ownership dimension weight
                Column 4: Irreplaceability dimension weight
                Column 5: Permenance of Impact dimension weight
                Column 5: Interconnectivity weight factor

    Calculates Case Study-Based Correlated Measures
    Output: Returns harm array with the final column now filled with
            Individual-Level losses
    '''
```

```
    make_harm_array = np.array(harm_array)

    if make_harm_array.ndim == 1:
        size = len(make_harm_array)
        harm_array = np.reshape(make_harm_array,(1, size))

    else:
        harm_array = make_harm_array

    r_weights = regime_distros[:,1].astype(int)

    for j in range(len(harm_array)):
        select_regime = random.choices(regime_distros[:,0], weights =
                                       (r_weights), k=1)
        #print("selected regime:", select_regime)
        rand_regime = np.array(select_regime)

        for i in range(len(regime_distros)):
            if rand_regime == regime_distros[i][0]:
                #print("regime match: ", regime_distros[i][0])
                w_own = float(regime_distros[i][2])
                #print("w_own:", regime_distros[i][2])
                w_irrep = float(regime_distros[i][3])
                #print("w_irrep", regime_distros[i][3])
                w_perm = float(regime_distros[i][4])
                #print("w_perm:", regime_distros[i][4])
                w_intercon = float(regime_distros[i][5])
                #print("w_intercon:", regime_distros[i][5])

                harm_array[j][2] = (float(harm_array[j][0])) *
                (.01 * ((w_own + w_irrep + w_perm)* w_intercon))

                break

    return harm_array

### Setup ###

ds_years = ## insert time interval for rate-paraemter here ##
simulations = ## insert simulations ##

df = pd.read_csv(## insert csv file here ##)
### Import data here ###
## Data should be a csv file of incident data with the following
columns:
    # Column 1: Individual Cyber Harm related to incident
    # Column 2: Reserved for any notes/additional details you want
imported
    # Column 3: Public Service Impacted, if using municipalities.
```

```
                # Otherwse, leave blank
    # Column 4: Entity-level cost
    # Column 5: Bottoms-up individual level cost calculation.
                # This can be blank if you are able to use the
                # Case Study-Based Method.

print(df)
claims_data = df.to_numpy()
print(claims_data)

econ_array = []
safesec_array = []
rep_array = []
psych_array = []
uncat_array = []
agg_array = []

### Organize imported data by Harm Type from the Taxonomy ###

for claimscount in range(len(claims_data)):

    new_claim = [claims_data[claimscount][0],
claims_data[claimscount][3],
                 claims_data[claimscount][4],0]
    # print("this is new_claim", new_claim)

    if new_claim[0] == 'Economic':
        new_claim.pop(0)
        if len(econ_array) == 0:
            econ_array = new_claim
        else:
            econ_array = np.vstack([econ_array, new_claim])

    elif new_claim[0] == "Safety & Security":
        new_claim.pop(0)
        if len(safesec_array) == 0:
            safesec_array = new_claim
        else:
            safesec_array = np.vstack([safesec_array,new_claim])

    elif new_claim[0] == "Reputational":
        new_claim.pop(0)
        if len(rep_array) == 0:
            rep_array = new_claim
        else:
            rep_array = np.vstack([rep_array, new_claim])

    elif new_claim[0] == "Psychological":
        new_claim.pop(0)
```

```
            if len(psych_array) == 0:
                psych_array = new_claim
            else:
                psych_array = np.vstack([psych_array, new_claim])

        else:
            new_claim.pop(0)
            if len(uncat_array) == 0:
                uncat_array = new_claim
            else:
                uncat_array = np.vstack([uncat_array, new_claim])

        if len(agg_array ) == 0:
            agg_array = new_claim
        else:
            agg_array = np.vstack([agg_array,new_claim])

### Create Lambdas for each Harm Category ###
econ = Lambda_create (calc_IL2(econ_array, regime_distros_econ),
ds_years)
ss = Lambda_create (calc_IL2(safesec_array, regime_distros_econ),
ds_years)
rep = Lambda_create (calc_IL2(rep_array, regime_distros_econ),
ds_years)
psych = Lambda_create (calc_IL2(psych_array, regime_distros_econ),
ds_years)
agg = Lambda_create (calc_IL2(agg_array, regime_distros_econ),
ds_years)

### Run Simulations ###
plot_MonteCarlo (econ, ss, rep, psych, agg, simulations)
```