Conceptualizing Human Resilience in the Face of the Global Epidemiology of Cyber Attacks

L Jean Camp, Marthie Grobler, Julian Jang-Jaccard, Christian Probst, Karen Renaud, Paul Watters
ljeanc@gmail.com, Marthie.Grobler@data61.csiro.au, j.jang-jaccard@massey.ac.nz, k.renaud@abertay.ac.uk, P.Watters@latrobe.edu.au

Abstract

Computer security is a complex global phenomenon where different populations interact, and the infection of one person creates risk for another. Given the dynamics and scope of cyber campaigns, studies of local resilience without reference to global populations are inadequate. In this paper, we describe a set of minimal requirements for implementing a global epidemiological infrastructure to understand and respond to large-scale computer security outbreaks. We enumerate the relevant dimensions, the applicable measurement tools, and define a systematic approach to evaluate cyber security resilience. From the experience in conceptualizing and designing a cross-national coordinated phishing resilience evaluation, we describe the cultural, logistic, and regulatory challenges to this proposed public health approach to global computer assault resilience. We conclude that mechanisms for systematic evaluations of global attacks and the resilience against those attacks exist. Coordinated global science is needed to address organised global ecrime.

1. Introduction

There are multiple approaches to understanding the diffusion and flow of cyber attacks, such as eCrime and malware propagation across the Internet. One approach is the modeling of the overall system to understand the interactions of different components of systems and networks [1]. Regardless of the approach taken, the human element is typically perceived to be the weakest link within socio-technical systems that are otherwise provably secure [2].

In this paper, we argue that there is a need to interweave the threads of complex modeling and human behavior in order to inform effective counter-responses to cyber attacks. Although our proposed approach builds on the epidemiological understanding of the health system, we assert that an accurate understanding of endemic attacks on computer networks and systems requires a theoretical component beyond the current reductionist approach often used in public health [3]. In the reductionist approach, attack detection, analogous to the detection of a specific disease is focused on raw data analysis, and individuals are modelled as identically, indistinguishable nodes. Public health models, as applied to computer security research, have focused on networks and systems, using the technical frame without the behavioral frame [4].

Our contribution to the theory of secure information systems is to motivate the need for a "cyber epidemiology" that treats individuals as highly distinct, independent, and important agents within a socio-technical system. Recalling that epidemiology deals with understanding the origins, incidence, and control measures for disease, whether social or physiological in origin [5], we advocate an approach to understanding how cybercrime thrives due to a failure to develop the understanding needed for effective behavioral control measures that are presented at the right place and the right time. These controls can only be determined once we understand the population distribution of behavioral risk factors, requiring a holistic, ecologically valid approach to engendering resilience and understanding location-specific vulnerability to social engineering attacks.

To make this contribution, we enumerate the critical dimensions of human behavior that have been identified in previous work [6]. Here, the focus is on individuals, and not on organizations or teams. This is to account for the issues of scope, not because we dismiss, in any way, the importance of addressing employee vulnerability in organizations, or the issue of collective decision-making. Addressing the effect of groups and teams will be interesting at a later stage in order to understand effects of policies and group influence.

As an argument for feasibility, we identify a subset of the available tools and datasets that are needed to meet this challenge. Acknowledging the challenges of this approach, we include a short exposition of some

URI: https://hdl.handle.net/10125/59914
ISBN: 978-0-9981331-2-6

of the global research challenges for investigating the human dimension of cyber epidemics. This is combined with a multi-national pilot of an online resiliency benchmarking experiment. We finally sketch our vision for how the data collected from our experiment can be used.

2. Motivation

Attacks using the Internet are endemic. They have been modeled as epidemics, with interactions between phishing, infected servers, and spam, all embedded in a single model. In 1999, White first introduced a conceptual model of the Internet as a biological system, where it is never the case that everyone is in perfect health [7]. Newman, Forrest and Balthrop took the general model and expanded it to the specific case of email in 2002 [8]. From then on, the most common approach to complex modeling of threats on the Internet is to treat humans as homogeneous, or, as *per* the public health classification, identically, indistinguishable nodes.

Building on this example, humans on the network are simply an exogenous force that interacts with the network, like electricity, beyond the scope of accurate integration with a dynamic model. Under the scale-free model of the network, the routers themselves were theorized out of existence [9], much less humans or our individual or collective behaviors. There is currently a major investment in understanding the technical scale of attacks (see the Internet Measurement Conference [1], and [10, 11]), as well as investments in understanding the scale and patterns of diffusion of online attacks [12]. Yet the inclusion of different types or groups of humans is relatively rare, with some notable exceptions [13].

Modeling of network threats has moved away from unrealistic scale-free conceptions of networks, and is now grounded in realistic measures and distributions of observable technical phenomena [14, 15]. However, the human element within a cyber attack contributes a certain variability in which the true online risk resilience remains unpredictable. This previous static approach has now given way to more realistic measurements and topology [16, 17], informing the need for realistic and more nuanced models of human risk perception and behavior. Most human subject studies, however, carry out explorations with using controlled A/B tests implemented once, with limited feedback [18, 19, 20].

Epidemiological modeling is in another academic silo addressing heterogeneity in time zones [21], software and hardware components [22], or modeling the location of the human as an important component of device interaction [23]. Models of malware that have included human behavior have provided large-scale generalizations in terms of modeling agents [24]. For example, one malware model distinguished between “careful” and “careless” populations, this generating the overall dynamics of an epidemic that matched observed behavior [17]. Despite the varying research directions and approaches, no all-encompassing logic was identified that underlies the model of how these human behaviors were associated with the generation of the critical variable of the likelihood of being subverted, other than that some populations are more, or less, resilient to attack.

It has been found that different types of threats can materialize in certain domains. A single attack type can be characterized in vastly different ways, dependent on the requirements and specifications of both the attacker and the defender. For example, social engineering attacks are highly optimized and targeted by attackers [25] while defenders still engage in rough categorizations of the attack [26]. Cyber-social systems [27] are a new abstraction method to consider human actors, virtual and physical infrastructure, and even society and policies in this categorization. They lift socio-technical systems to the societal level, enabling reasoning about actors, policies, attacks, and attacker strategies.

Our contribution to theory is the proposal for a systematic use of consistent tested mechanisms that are reported in a consistent manner. The goal is to enable complementary, systematic investigations that reflect extant understanding of resilience to social engineering, that can be improved with the inclusion of new data over time. Such an approach could be used as a component to inform models of attack diffusions that combine social engineering and technical components, or as a prerequisite for informing experiments related to interventions that lead to change, or as a source for analytic nuance when populations are known but all dimensions have not been tested. The ultimate goal is to be able to identify the most vulnerable populations, and use that to craft interventions that can limit the spread of malware via the human agent.

3. Critical Indicators

There are extant tools to measure susceptibility and resilience [28]. These are not yet perfect, and there is an on-going argument on improving surveys and questionnaires versus using less-refined but more consistent measures. Unlike improvement in physical measurements, one cannot simply improve

[1] https://www.sigcomm.org/events/imc-conference

the accuracy of measurement while maintaining efficacy of comparisons with previous work. In reality, slight changes in bias make it nontrivial to compare the accuracy of improved tools with previous versions.

As with public health classification systems, it is critical to obtain the correct data and target the right samples of "at risk" populations in order to detect an epidemic-scale risk. Yet, in the online world, we do not yet know which populations to sample, or how populations differ in terms of susceptibility to online infections. To use the illness metaphor, we may be sampling only the retirement communities or only the fitness clubs, and thus missing the bigger picture in our attempts to understand user-centered online attacks. In studies conducted globally there are no persistent results on even basic cyber risk indicators. The study by Van De Weijer and Leukfeldt [29], for example, found no relationship between the "big five" personality factors and cybercrime victimization, beyond general crime victimization. In contrast, we still need to characterize the interaction of cognition, experience, demography, and stress. Studies in cultural susceptibility are inchoate, as online risk resilience may be affected by a variety of factors, although explanatory models are emerging in recognized hot-spots, such as Sub-Saharan Africa which is the home of 419 or "Nigerian Scams" [30].

Previous studies identify factors but are inconclusive as to what their influence is; factors found to impinge perception of phishing resilience include demographic factors, specifically gender, age, education, income, routine activities, computer experience, and baseline risk preferences. When offline, for example, women are found to be more risk averse and perceive higher risk than for online activities [31]. Educated individuals should theoretically be more risk averse, as they are more informed. Conversely, the educated may perceive of these risks as well-understood and thus less concerning (as described in the following section on risk perception). Wealthier individuals should arguably have a greater perception of online risks, as they have more assets to protect, alternatively they may have a greater ability to recover, and thus be less concerned about phishing. Older adults may have a different understanding of technology compared to younger cohorts [32], and risk communication needs to be aligned the episodic cognition to be effective with older populations [33].

Information security practices are often driven by privacy concerns and may be affected by privacy preferences. Experienced users may be better informed, consider security risks to be less novel, and assume that the hazard impacts the general public and not just the individual. The impact of demographic variables may disappear when we account for routine activities such as time spent online and online purchases made. We need consistent methodological "security health" measurement tools that can be used and refined across regions and cultures. Experimental methods can eliminate social desirability and other biases inherent in questionnaire-based studies, and therefore likely play a growing and significant role. A study by Graves *et al.* [34], for example, experimentally manipulated key variables in measuring attitudes to cybercrime judgements, including attack motivation, scope, and value. Canetti *et al.* [35] used simulated cyber attacks to measure changes in cortisol levels of victims, but necessarily focused on a small population.

4. A Health Resilience Model

To address the very real interaction of human and technical vulnerabilities of the network, realistic distributions of human behavior are needed. Unlike machines, humans are highly distinctive and not perfectly reproducible. Here, we propose a model of populations that enables statistical characterizations in order to create an empirical yet realistic estimate of human behavior.

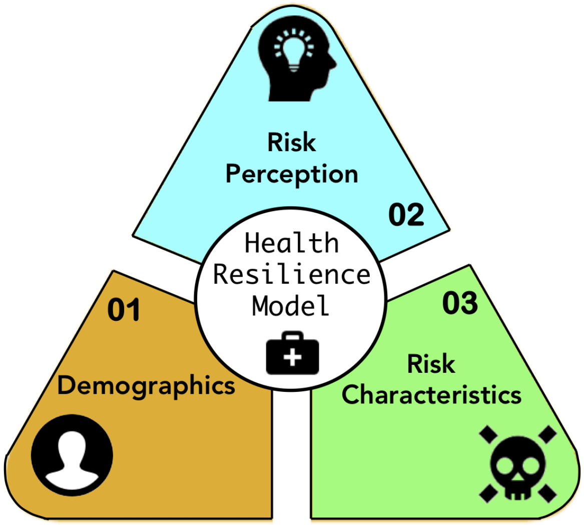

Figure 1. Health Resilience Model

In the initial piloting of the proposed model, we developed a cross-national coordinated phishing resilience evaluation program in which we built on three main dimensions of resilience as underlying factors (Figure 1): (1) demographics, (2) risk perception and (3) risk characteristics. These factors are the foundation identified in the striving to formalize an online risk epidemiology. The aim of this cross-national resilience evaluation is to build a global baseline for identifying and extrapolating factors that contribute to increased vulnerability to online risk behaviors, or conversely, contribute to a more acute online risk resilience. We will test this model through a global experiment within various representative target audiences.

We now detail the identified dimensions that may impinge an individual's resilience to phishing and contribute to the overall risk factor within human use of technology systems. These are the dimensions that we isolated as most pertinent in determining the security health of a human interacting with the online world.

(1) Demographics, in terms of people that fall victim to phishing attacks is the most direct way of finding the human in the global epidemiology of cyber security. However, in this sense, humans can definitely be seen as endogenous, with no single source of external or environmental attribute contributing, in isolation, to increased online risk.

Previous research on phishing has been inconsistent in delivering reliable results. Studies show that adolescents differ from other populations in legitimate technology use [36], with a younger population (18–25) being the most susceptible to online deception, despite being described as the most technologically enhanced generation [31]. Women are traditionally more risk averse [37] and therefore the extrapolation is that female populations would perceive a greater threat from computer security risks. However, research results vary from gender having no impact [38], to being inversely proportional to susceptibility [39], to being correlated with susceptibility [40].

Despite the need for investigations into cyber resilience [41] and there currently being no conclusive, corroborative research results regarding the link between demographics and risk resilience, there seem to be visible links between an increased risk resilience and certain demographic elements, as detailed above.

Demographics are pertinently included as a dimension in the health resilience model despite prior inconclusive results due to the relative weight that demographical factors have in terms of socio-technical approach, and the perceived influence of demographical factors on risk perception. Similar to the public health model, demographic factors do not play a leading role in the vast majority of health approaches, but there are definite instances in which demographic factors will lead to an increased risk of infection. These links are encapsulated in the demographics dimension and need to be investigated on a global platform in order to identify pervasive links. In our cross-national coordinated phishing resilience evaluation experiment, we included a number of demographic differentiators, but also included comprehension of English as language as common denominator to facilitate the program at a provenance level.

(2) Risk Perception, both online and offline, is influenced by several factors. The foremost of these factors are characteristics of the hazard and availability of risk information. In addition, routine activities, such as frequency of Internet use or financial transactions online, also increase the overall perceived online risk. This may be because a higher incidence of routine activities correlates with a greater probability of cybercrime victimization.

In our cross-national experiment, we provide control for the hazard and availability of risk information by presenting participants with selected websites in an image context that prevents participants from clicking on any links, or from engaging in other evaluations that could affect the validity of the experiment. To simulate the effect of theory versus practice application, the presented website images have different levels of familiarity for the different geographical audiences,i.e., we include both international and regional websites.

The experiment execution is carefully balanced with a time limitation and a targeted bonus compensation as an additional stress factor. This aims to discourage experiment participants from either selecting actions at random (logging in at a safe website or navigating away from a perceived dangerous website), or taking an unrealistically long time period to determine the correct action to be selected. This increased focus on the severity of the risk (albeit there is a time penalty if an incorrect action is selected) may address those who perceive phishing as a low risk activity.

(3) Risk Characteristics often impinge perceived risk. The perceived risk of controlled information sharing, for example, is different from mandatory information disclosure. Control in this sense, is used as a term of art from the canonical studies of risk perception by Slovic [42], indicating whether individuals can act to mitigate the harm once exposed to the risk. In our first set of experiments, we examine risk where the user cannot control what happens to information after it is disclosed – specifically by making the decision to authenticate. This is contrasted to voluntariness, where engaging in the activity is a free choice by the participant: smoking, for example, is voluntary, while air pollution is not. Risk perception has been applied to online risks, including phishing, but generally not integrated into resilience studies [43].

5. Tools and Techniques

The factors discussed above have been investigated in other research studies, but in an inconsistent manner. In this section, we discuss some of the available tools from usable security, psychology, and economics that have been used in terms of online risk resilience evaluation.

The **Balloon Analogue Risk Test (BART)** instruments risk posture [44] in response to the identified failure in the Pratt Arrow questions. BART has been shown to consistently align with risk posture, through comparison with other instruments and repeated tests of the same people in different conditions. Participants in the test should judge the risk of inflating a simulated balloon without popping it. The premise of this test applied to online risk resilience is that people who are in general more risk-seeking will most likely be less resilient to social engineering. Thus, the focus of online resilience building should be focused on those engaged in high-risk behaviors. Investments in education could be combined with campaigns in harm reduction for risk-seeking populations.

The **Internet Users Privacy Information Concerns (IUPIC)** is a repeatedly validated survey instrument that uses groups of questions and scenarios. It has been used by well over a thousand researchers to evaluate the privacy posture of Internet users [45]. The tool consists of a set of simple Likert queries, *e.g.*, "Online companies should devote more time and effort to preventing unauthorized access." Those are categorized as general awareness of privacy practice, perceptions of the reliability and integrity of online data, concerns about unauthorized secondary use, awareness of the potential for improper access, and global information privacy concerns. These are followed by two scenarios with more of less sensitive information, for which participants are queried.

The **Simple Usability Scale (SUS)** is the most common tool for usability experiments [46]. This is a set of questions using a ten point Likert scale focusing on measuring subjective usability. However, usability of a security tool is not necessarily a good measure of its efficacy. A tool may be perceived as usable without protecting the individual, as is far too abundantly illustrated by the proliferation of fake anti-virus software. Fake anti-virus software is software that is sold as protection, but actually installs malicious code on the buyer's machine. It is most often distributed through cold calling by fraudsters pretending to be from major IT companies, or through deceptive online advertisements.

The standard **Task Load Index (TLX)** measures the subjective perceptions of usability and acceptability [23]. It was developed by the Human Performance Group at NASA's Ames Research Center and builds on insights from more than 40 laboratory simulations. The TLX measures mental, physical, and temporal demands of a task. It measures self-perceptions of efficacy to determine if individuals' believe that they are successful is aligned with actual success. The applications to phishing are obvious.

The **Security Behavior Intention Scale (SEBIS)** evaluates both intention and behavior, which may not always align [47]. This is a scale of sixteen Likert-style items. It measures attitudes towards choosing passwords, device securement, staying up-to-date, and proactive awareness.

The **End-User Expertise Instrument** [48] is a set of questions that have been coded and validated. The question evaluates people as having more or less computer and security expertise. This tool characterises people into three categories based on knowledge, experience, and skills: high computer and security expertise; high computer and low security expertise; or low computer and security expertise.

The **Nine-Dimensional Canonical Risk Dimensions** was initially introduced to address perceptions of environmental risk in 1979 [42]. It has been used widely in a range of domains [49] and has now been adopted in online risk perception [39, 50]. Fischhoff *et al.* [51] used the psychometric paradigm of expressed preferences and identified nine orthogonal characteristics of hazards that determine their perceived risk. *Immediacy* reflects whether the consequences of an activity are delayed or immediate; *e.g.*, stress relief from smoking is immediate, while the lung cancer may be delayed. *Knowledge to the exposed* refers to an individual's perception of understanding of an activity; *e.g.*, the majority of individuals would consider themselves to be better than average drivers, though that is not statistically possible. The knowledge to the exposed could result in more educated individuals perceiving online behaviors as less risky. *Knowledge to science* enumerates the perceived knowledge of experts and/or the effectiveness of expert systems; *e.g.*, end-users often (incorrectly) believe that anti-virus software stops 100% of all malware. *Control* (as previously discussed) indicates whether individuals feel they can control the consequences of an activity; *e.g.*, individuals often feel safer driving than flying because they feel to have more control when driving. *Newness* reflects whether a risk is perceived to be new or old; *e.g.*, high fructose corn syrup is perceived to be new and thus more harmful than its counterpart cane sugar. *Common-dread* refers to whether the risk is commonly encountered or rarely experienced; *e.g.*, risks such as crossing the road are commonplace and ignored by most individuals. *Chronic-catastrophic* indicates scale, *i.e.*, whether the risk impacts one entity at a time or large numbers of people at once. If an educated person has an awareness of the risk of large-scale cyber attacks, then being more educated may correlated with a higher perception of risk. Finally, *severity* indicates the magnitude or intensity of the consequences of a risk.

These tools and techniques all play some part in the experimental design of the health resilience model.

6. Global Demographic Characterizations

Due to the global nature of our cross-national resilience evaluation experiment, a number of challenges emerged. This section details the cultural, logistic, and regulatory challenges that played a major role in the design and the successful pilot of the experiment.

Cultural Differences: Previous work has found substantive differences between countries. Security as well as privacy in social aspects have primarily focused on 'Western, Educated, Industrialized, Rich and Democratic' (WEIRD) societies. For instance, privacy risk perceptions of American and German participants were found to be higher than their Chinese counterparts [52], possibly due to stricter privacy laws [53, 54, 55]. Hence, WEIRD populations are not necessarily representative of other populations in terms of behavioral research [56], nor representative in terms of the user base of some online communication platforms, *e.g.*, WhatsApp [57]. This has been further exemplified by research on mobile phone sharing practices in Bangladesh [58].

Prior research has shown that security and privacy concerns of internet users vary across different cultural and political settings, as well as level of user expertise [59, 60]. An early study of social media privacy attitudes and behavior in India used a survey of 407 participants [61]. The design was grounded in similar surveys that included only American participants [62]. Indian participants were found to have high levels of trust in information disclosure in the public and private sectors, which sharply contrasted with privacy attitude of participants in the United States. This is also illustrated in information exposure in daily life. For example, the posting of students' grades along with their full names on physical, publicly visible departmental noticeboards is common in India, and even those published on websites have low security [63].

The differences between countries and the lower level of privacy concern in India were further reified by cross-cultural research on privacy by Wang *et al.* [64]. However, research in risk perceptions on various other social media platforms, including Friendster, MySpace, and Facebook, has reported weak correlations between users' privacy choices and their online behavior [65]. Privacy preferences, measured using a standard Likert scale, were found to be significant but to have the least impact on behavior [66].

Studies of eCrime, both of perpetrators and victims, have found global variance based on nation and region of origin. Empirical analysis led by Kanich [67] examined the value chain in pharmaceutical spam, and found that different parts of the value chain were concentrated in different global hot spots. Two Caribbean payment service providers handled most of the payments; Indian pharmaceutical companies filled orders; Chinese businesses provided bullet-proof DNS services; and Russia was the home of the coordinating affiliate programs. This technical analysis enabled an enforcement response, greatly decreasing the prevalence of pharmaceutical spam. An early macroeconomic analysis of spam looked at the role of ISPs and included variables from the governance of the nation associated with the ISP. In that work, van Eeten *et al.* [68] considered the efficacy of specific industry and national policies in the spam ecosystem. Generic spam has been subject to significant economic analysis. Nation and region of origin have been found to be relevant in analyses of spam [69, 70]. The economics of malware illustrates the significance of state-level variables, including the economic variables we consider in the following [71, 72].

Cultural Challenges: Cultural sensitivities are necessary for developing appropriate research instruments. For example, studies of privacy have found different patterns of concern in different countries [73]. None of these are unique to studies of computer security; however, a summary for the computer security community may be of use. In this particular study, the initial work was implemented in the United States, where the basic demographic questions are gender, race, age, income, and education. These could not be directly translated to the five nations participating in our experiment.

In terms of gender, the US questions presented participants with two options: 'Male' or 'Female'. Amidst sensitivities and recent privacy legislation enacted in the European Union and Australia, a third option was included: 'Prefer not to say'. This enables individuals to opt out of providing their sensitive data, as the new legislation mandates. The inclusion of the third option does make it more difficult to draw substantial conclusions related to gender on online risk resilience behavior.

Language was another cultural challenge we faced in designing the experiment. The English language was selected as common denominator for the pilot to ensure a sound experiment that was not influenced by possible ambiguities introduced by translation. Therefore, being able to read and understand written English was a prerequisite for participating in the study. One of the demographically aligned questions in the experiment asked participants to select all the languages that they can speak. Due to cultural diversity and global migration rates, it became rather difficult to include all the main languages that could possibly represent the participant group. For example, South Africa has 11 official languages, Australia has more than 200 community languages, and New Zealand has 3 official languages [74]. In Los Angeles alone, citizens can register to vote in ten languages, as there is no national language in the United States. These numbers do not include the home languages of all communities of migrants or communities indigenous to these countries.

Logistic Challenges: A significant logistical challenge for a cross-national evaluation pilot like ours relates to difference in legal requirements for data storage, data protection, legitimacy of researchers, and last but not least for data sharing.

Also, an innocent aspect such as studying groups with highly variable income means that any payment sufficient to motivate a participant from a wealthier country may be biasing for a participant from a less well-off country. Payment motivation is a complex psychological phenomenon which reflects the absolute and relative differences in purchasing power between individuals in different countries, let alone within those countries. Carr and MacLachlan [75] found that motivation to complete tasks could be reduced where low-paid workers performed the same task as high-paid workers. Crucially, the demotivating effect were found to be double, since both high-paid and low-paid workers experienced decreased work motivation. Payment across borders to different participant groups needs to take this into consideration, especially where the payment rates are made public and must be approved by the institutional review bodies at each location.

Regulatory Challenges: Institutional Review Boards provide a minimal level of protection for all participants. In this experiment, research ethics enforces the application of ethical principles across the international investigation of human subjects as main focus of the online resilience test. With the involvement of different countries, and different institutions within those countries, it becomes constraining to adhere to the different requirements and prescriptions. Some institutions posed a lengthy processing time for applications, some required a substantially detailed experiment design before submission, and others had a lighter touch.

7. Vision and Limitations

Understanding prevalence and efficacy of global attacks requires global, cumulative data. There are strong reasons for sharing data, yet sometimes the sheer mass of data makes it difficult for those with innovative ideas to test and model. The use of a consistent set of measures enables the sharing of informed distributions that can be compared with other data. This may be more valuable than the data sharing itself.

Currently, to model network vulnerability to inadvisable human behaviors, it is necessary to configure an experiment, complete the analysis and publish as a stand-alone analysis. The next study of human behavior would similarly compile results and a control group as a comparison. Consider, instead, a shared data ethos where there is a range of well-described parameters about human behaviors using empirical methods from peer-reviewed publications, without requiring any contribution of raw data from the participants. With this approach, innovations in human behaviors can be easily compared for more precise measures of the global population reflecting the realities of the new millennium. Control groups can be compared to the information about other control groups, and correlations based on demographics can add nuance to smaller qualitative results.

Generally, each research publication includes data on the number of participants of the study, the choices of each participant, and the demographics of these participants. Yet the detailed data themselves are not available for comparisons, or analyses that update our understanding of human behavior to be more precise by combining these data because of human subject concerns. Individual research products are often stand-alone, difficult to repeat, and published as an atomic complete piece. However, the parameters of the distributions could be made available without such risk.

Each researcher who engages in qualitative research begins the process of developing a mobile privacy codebook from his or her data from scratch. Every researcher has their own control group and Bayesian prior. A challenge we do not address here is how to provide parameterization, resource identifiers (DOI) and basic analyses so that it is possible to answer questions through metadata analysis. Systematic data creation and tools are arguably a precondition for this. Such analysis today is painstaking and grounded in individual literature searches.

The example of human behavior with respect to phishing resilience shows how better sharing of parameters could create a baseline for long term data analysis and improved evaluation of individual results through research creation of baselines from previous work. This provides a case where previous results on human behaviors can be used to predict large-scale network responses to possible incidences. Our aim is a health resilience model to empower researchers on a global platform to do exactly this.

8. Conclusion

In this work we have argued for a systematic data-driven approach modeled on the understanding of public health challenges. We note that today the underlying dynamics are not well understood. To use the health metaphor, we could be tracking illnesses and epidemics by only looking into the day cares and hospitals, thus significantly over-counting events. Alternatively we may be looking in the fitness centers, thus seriously under-estimating the levels of illnesses and epidemics. The interaction of individual and cultural dimensions with phishing resilience are not well understood.

We conclude that this is a difficult but feasible way forward. What is required is a commitment by the involved research communities to share aggregate data and experimental platforms to facilitate a more accurate global comparison on online risk resilience. This will move us away from research products that are stand-alone and difficult to repeat, and will provide more valuable insight in terms of global resilience and where interventions are required.

Our vision is to use a set of well-understood, well-documented, and systematically used methods to explore phishing resilience. This could be a single platform for experimental implementation, with customization for each site, ideally including more aggressive sharing of metadata. In this paper, we illustrate that the scientific foundation exists, and that the larger structures needed to support this are possible, making a common platform for experimental implementation feasible, that can be customized by researchers.

Monitoring the health of cyberspace, like modeling the health of humanity ourselves, is not beyond the realm of the possible given the extant underlying understanding and the tools available today.

References

[1] E. Paja, F. Dalpiaz, and P. Giorgini, “Modelling and reasoning about security requirements in socio-technical systems,” *Data & Knowledge Engineering*, vol. 98, pp. 123–143, 2015.

[2] E. Ceesay, K. Myers, and P. Watters, “Human-centred strategies for cyber-physical security,” *EAI Endorsed Transactions on Security and Safety*, vol. 18, no. 4, p. e5, 2018.

[3] O. Hankivsky, L. Doyal, G. Einstein, U. Kelly, J. Shim, L. Weber, and R. Repta, “The odd couple: using biomedical and intersectional approaches to address health inequities,” *Global Health Action*, vol. 10, no. sup2, p. 1326686, 2017.

[4] H. Fryer, “The public health analogy in web security,” Ph.D. dissertation, University of Southampton, 2016.

[5] R. S. Bhopal, *Concepts of epidemiology: integrating the ideas, theories, principles, and methods of epidemiology*. Oxford, U.K.: Oxford University Press, 2016.

[6] P. Watters, “Investigating Malware Epidemiology and Child Exploitation Using Algorithmic Ethnography,” in *Proceedings of the 51st Hawai’i International Conference on System Sciences*, The Big Island, Hawai’i, 2018.

[7] T. White, B. Pagurek, and A. Bieszczad, “Network modeling for management applications using intelligent mobile agents,” *Journal of Network and Systems Management*, vol. 7, no. 3, pp. 295–321, 1999.

[8] M. E. Newman, S. Forrest, and J. Balthrop, “Email networks and the spread of computer viruses,” *Physical Review E*, vol. 66, no. 3, p. 035101, 2002.

[9] R. Pastor-Satorras and A. Vespignani, “Epidemic spreading in scale-free networks,” *Physical Review Letters*, vol. 86, no. 14, p. 3200, 2001.

[10] M. Uma and G. Padmavathi, “A Survey on Various Cyber Attacks and their Classification,” *IJ Network Security*, vol. 15, no. 5, pp. 390–396, 2013.

[11] G. Rattray and J. Healey, “Categorizing and understanding offensive cyber capabilities and their use,” in *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for US Policy*, 2010, pp. 77–97.

[12] D. Canali and D. Balzarotti, “Behind the scenes of online attacks: an analysis of exploitation behaviors on the web,” in *20th Annual Network and Distributed System Security Symposium, (NDSS) February 24-27*, San Diego, USA, 2013.

[13] M. Bashir, C. Wee, N. Memon, and B. Guo, “Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool,” *Computers & Security*, vol. 65, pp. 153–165, 2017.

[14] K. Ingols, M. Chu, R. Lippmann, S. Webster, and S. Boyer, “Modeling modern network attacks and countermeasures using attack graphs,” in *Computer Security Applications Conference, (ACSAC’09)*, 2009, pp. 117–126.

[15] V. Dutt, Y.-S. Ahn, and C. Gonzalez, “Cyber situation awareness: modeling detection of cyber attacks with instance-based learning theory,” *Human Factors*, vol. 55, no. 3, pp. 605–618, 2013.

[16] N. Husted and S. Myers, "Why Mobile-to-mobile Wireless Malware Won't Cause a Storm," in *Proceedings of the 4th USENIX Conference on Large-scale Exploits and Emergent Threats*, ser. LEET'11. Berkeley, USA: USENIX Association, 2011, pp. 7–7.

[17] T. Kelley and L. J. Camp, "Online promiscuity: Prophylactic patching and the spread of computer transmitted infections," in *The Economics of Information Security and Privacy*. Springer, 2013, pp. 157–180.

[18] R. Shillair, S. R. Cotten, H.-Y. S. Tsai, S. Alhabash, R. LaRose, and N. J. Rifon, "Online safety begins with you and me: Convincing internet users to protect themselves," *Computers in Human Behavior*, vol. 48, pp. 199–207, 2015.

[19] M. Junger, L. Montoya, and F.-J. Overink, "Priming and warnings are not effective to prevent social engineering attacks," *Computers in Human Behavior*, vol. 66, pp. 75–87, 2017.

[20] J.-W. H. Bullée, L. Montoya, W. Pieters, M. Junger, and P. H. Hartel, "The persuasion and security awareness experiment: reducing the success of social engineering attacks," *Journal of Experimental Criminology*, vol. 11, no. 1, pp. 97–115, 2015.

[21] D. Dagon, C. C. Zou, and W. Lee, "Modeling Botnet Propagation Using Time Zones," in *Network and Distributed System Security Symposium (NDSS)*, vol. 6, San Diego, USA, 2006, pp. 2–13.

[22] A. Alexeev, D. S. Henshel, M. Cains, and Q. Sun, "On the malware propagation in heterogeneous networks," in *12th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 17-19 October, New York, USA, 2016, pp. 1–5.

[23] J. O. Kephart and S. R. White, "Directed-graph epidemiological models of computer viruses," in *Computer Society Symposium on Research in Security and Privacy*. Oakland, USA: IEEE, 1991, pp. 343–359.

[24] S. Peng, S. Yu, and A. Yang, "Smartphone malware and its propagation modeling: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 2, pp. 925–941, 2014.

[25] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks," *Journal of Information Security and Applications*, vol. 22, pp. 113–122, 2015.

[26] C. F. M. Foozy, R. Ahmad, M. F. Abdollah, R. Yusof, and M. Z. Mas'ud, "Generic taxonomy of social engineering attack and defence mechanism for handheld computer study," in *Malaysian Technical Universities International Conference on Engineering & Technology, Batu Pahat, Johor*, 2011.

[27] J. Perno and C. W. Probst, "Behavioural profiling in cyber-social systems," in *The Fifth International Conference on Human Aspects of Information Security, Privacy and Trust*, Vancouver, Canada, 9 - 14 July, 2010, pp. 507–517.

[28] R. Heeks and A. Ospina, "Conceptualising the link between information systems and resilience: A developing country field study," *Information Systems Journal*, 2018.

[29] S. G. van de Weijer and E. R. Leukfeldt, "Big five personality traits of cybercrime victims," *Cyberpsychology, Behavior, and Social Networking*, vol. 20, no. 7, pp. 407–412, 2017.

[30] S. Ibrahim, "Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals," *International Journal of Law, Crime and Justice*, vol. 47, pp. 44–57, 2016.

[31] K. Coronges, R. Dodge, C. Mukina, Z. Radwick, J. Shevchik, and E. Rovira, "The influences of social networks on phishing vulnerability," in *45th Hawai'i International Conference on System Science (HICSS)*, Maui, Hawai'i, 2012, pp. 2366–2373.

[32] C. Lee and J. Coughlin, "Perspective: Older adults' adoption of technology: an integrated approach to identifying determinants and barriers," *Journal of Product Innovation Management*, vol. 32, no. 5, pp. 747–759, 2015.

[33] V. Garg, L. Lorenzen-Huber, L. J. Camp, and K. Connelly, "Risk communication design for older adults," in *ISARC. Proceedings of the International Symposium on Automation and Robotics in Construction*, vol. 29. Vilnius Gediminas Technical University, Department of Construction Economics & Property, 2012, p. 1.

[34] J. Graves, A. Acquisti, and R. Anderson, "Experimental measurement of attitudes regarding cybercrime," in *13th Annual Workshop on the Economics of Information Security. Pennsylvania State University*, 2014.

[35] D. Canetti, M. Gross, I. Waismel-Manor, A. Levanon, and H. Cohen, "How cyberattacks terrorize: cortisol and personal insecurity jump in the wake of cyberattacks," *Cyberpsychology, Behavior, and Social Networking*, vol. 20, no. 2, pp. 72–77, 2017.

[36] E. Hargittai and A. Hinnant, "Digital inequality: Differences in young adults' use of the Internet," *Communication Research*, vol. 35, no. 5, pp. 602–621, 2008.

[37] C. C. Eckel and P. J. Grossman, "Men, women and risk aversion: Experimental evidence," *Handbook of Experimental Economics Results*, vol. 1, pp. 1061–1073, 2008.

[38] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android permissions: User attention, comprehension, and behavior," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*. ACM, 2012, p. 3.

[39] V. Garg and S. Niliadeh, "Craigslist scams and community composition: Investigating online fraud victimization," in *Security and Privacy Workshops (SPW)*, 2013, pp. 123–126.

[40] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions," in *SIGCHI Conference on Human Factors in Computing Systems*, 2010, pp. 373–382.

[41] D. Gerber *et al.*, "ASIC calls for health check on cyber resilience," *Governance Directions*, vol. 67, no. 4, p. 232, 2015.

[42] P. Slovic, B. Fischhoff, and S. Lichtenstein, "Rating the risks," *Environment: Science and Policy for Sustainable Development*, vol. 21, no. 3, pp. 14–39, 1979.

[43] T. Halevi, N. Memon, and O. Nov, "Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks," 2015, https://ssrn.com/abstract=2544742.

[44] C. W. Lejuez, J. P. Read, C. W. Kahler, J. B. Richards, S. E. Ramsey, G. L. Stuart, D. R. Strong, and R. A. Brown, "Evaluation of a behavioral measure of risk taking: the Balloon Analogue Risk Task (BART)," *Journal of Experimental Psychology: Applied*, vol. 8, no. 2, p. 75, 2002.

[45] N. K. Malhotra, S. S. Kim, and J. Agarwal, "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model," *Information Systems Research*, vol. 15, no. 4, pp. 336–355, 2004.

[46] J. Brooke, "SUS-A quick and dirty usability scale," *Usability Evaluation in Industry*, vol. 189, no. 194, pp. 4–7, 1996.

[47] S. Egelman and E. Peer, "Scaling the security wall: Developing a security behavior intentions scale (sebis)," in *33rd Annual ACM Conference on Human Factors in Computing Systems*, 2015, pp. 2873–2882.

[48] P. Rajivan, P. Moriano, T. Kelley, and L. J. Camp, "What Can Johnny Do?–Factors in an End-User Expertise Instrument," in *HAISA*, 2016, pp. 199–208.

[49] P. Slovic, "Perception of risk: Reflections on the psychometric paradigm," 1992, https://scholarsbank.uoregon.edu/xmlui/handle/1794/22510.

[50] M. Harbach, E. Von Zezschwitz, A. Fichtner, A. De Luca, and M. Smith, "It's a hard lock life: A field study of smartphone (un) locking behavior and risk perception," in *SOUPS*, 2014, pp. 213–230.

[51] B. Fischhoff, P. Slovic, S. Lichtenstein, S. Read, and B. Combs, "How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits," *Policy Sciences*, vol. 9, no. 2, pp. 127–152, 1978.

[52] E. U. Weber and C. Hsee, "Cross-cultural differences in risk perception, but cross-cultural similarities in attitudes towards perceived risk," *Management Science*, vol. 44, no. 9, pp. 1205–1217, 1998.

[53] Rights, Family Educational and Act, Privacy, "USC 1232-34 CFR Part 99," 1974.

[54] S. Bennett, "GDPR: Change to European privacy laws and its impact on Australian businesses," *Governance Directions*, vol. 70, no. 2, p. 85, 2018.

[55] M. Cornock, "General Data Protection Regulation (GDPR) and implications for research," 2018.

[56] J. Henrich, S. J. Heine, and A. Norenzayan, "Most people are not weird," *Nature*, vol. 466, no. 7302, p. 29, 2010.

[57] Statistica, "Share of population in selected countries who are active WhatsApp users as of 3rd quarter 2017," 2018, https://www.statista.com/statistics/291540/mobile-internet-user-whatsapp/.

[58] S. I. Ahmed, M. R. Haque, J. Chen, and N. Dell, "Digital Privacy Challenges with Shared Mobile Phone Use in Bangladesh," in *PACM on Human-Computer Interaction, Vol. 1*, 2017.

[59] S. Bellman, E. J. Johnson, S. J. Kobrin, and G. L. Lohse, "International differences in information privacy concerns: A global survey of consumers," *The Information Society*, vol. 20, no. 5, pp. 313–324, 2004.

[60] P. van Schaik, J. Jansen, J. Onibokun, J. Camp, and P. Kusev, "Security and privacy in online social networking: Risk perceptions and precautionary behaviour," *Computers in Human Behavior*, vol. 78, pp. 283–297, 2018.

[61] B. Ur and Y. Wang, "A cross-cultural framework for protecting user privacy in online social media," in *Proceedings of the 22nd International Conference on World Wide Web*. ACM, 2013, pp. 755–762.

[62] P. Kumaraguru and L. F. Cranor, "Privacy indexes: a survey of Westin's studies," 2005, http://repository.cmu.edu/isr/856/.

[63] "Cornell Student Scrapes Indian Exam Results, Exposes the System's Flaws — Scientific American Blog Network," https://blogs.scientificamerican.com/guest-blog/cornell-student-scrapes-indian-exam-results-exposes-the-systems-flaws/, (Accessed on 06/14/2018).

[64] Y. Wang, G. Norice, and L. F. Cranor, "Who is concerned about what? A study of American, Chinese and Indian users' privacy concerns on social network sites," in *International Conference on Trust and Trustworthy Computing*, 2011, pp. 146–153.

[65] A. Acquisti and R. Gross, "Imagined communities: Awareness, information sharing, and privacy on the facebook," in *International workshop on privacy enhancing technologies*, 2006, pp. 36–58.

[66] V. Garg and L. Camp, "Ex ante *vs.* ex post: Economically efficient sanctioning regimes for online risks," in *TPRC 41: The 41st Research Conference on Communication, Information and Internet Policy*, 2013.

[67] C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. M. Voelker, V. Paxson, and S. Savage, "Spamalytics: An empirical analysis of spam marketing conversion," in *15th ACM conference on Computer and communications security*, 2008, pp. 3–14.

[68] M. Van Eeten, J. Bauer, H. Asghari, S. Tabatabaie, and D. Rand, "The role of internet service providers in botnet mitigation an empirical analysis based on spam data," in *The Ninth Workshop On The Economics Of Information Security (Weis 2010)*, 2010.

[69] Microsoft, "Microsoft security intelligence report," 2011, Https://Www.Microsoft.Com/En-Us/Download/Details.Aspx?Id=27605.

[70] V. Garg, T. Koster, and L. J. Camp, "Cross-country analysis of spambots," *EURASIP Journal on Information Security*, vol. 2013, no. 1, p. 3, 2013.

[71] M. J. van Eeten and J. M. Bauer, "Economics of malware: Security decisions, incentives and externalities," *OECD Science, Technology and Industry Working Papers*, vol. 2008, no. 1, p. 0_1, 2008.

[72] V. Garg and L. J. Camp, "Macroeconomic Analysis of Malware," in *20th Annual Network and Distributed System Security Symposium, (NDSS) February 24-27*, 2013.

[73] C. L. Miltgen and D. Peyrat-Guillard, "Cultural and generational influences on privacy concerns: a qualitative study in seven European countries," *European Journal of Information Systems*, vol. 23, no. 2, pp. 103–125, 2014.

[74] WorldAtlas, "What languages are spoken in Australia?" 2018, https://www.worldatlas.com/articles/what-languages-are-spoken-in-australia.html (Accessed 12 June 2018).

[75] S. C. Carr, D. McLoughlin, M. Hodgson, and M. MacLachlan, "Effects of unreasonable pay discrepancies for under- and over-payment on double demotivation," *Genetic, Social, and General Psychology Monographs*, 1996.