2021

Cyber Insurance Effects on Cyber Hygiene: Does the Homeostatic Effect Apply?

Wendi M. Kappers
Embry-Riddle Aeronautical University, kappersw@erau.edu

Aaron Glassman
Embry-Riddle Aeronautical University, glassf10@erau.edu

Michael S. Wills
Embry-Riddle Aeronautical University, wills004@erau.edu

Issues in Information Systems
Volume 22, Issue 4, pp. 1-8, 2021

DOI: https://doi.org/10.48009/4_iis_2021_1-8

Cyber insurance effects on cyber hygiene: Does the homeostatic effect apply?

Dr. Wendi M. Kappers, *Embry-Riddle Aeronautical University, kappersw@erau.edu*
Dr. Aaron Glassman, *Embry-Riddle Aeronautical University, glassf10@erau.edu*
Mr. Michael S. Wills, *Embry-Riddle Aeronautical University, Wills004@erau.edu*

Abstract

A theoretical framework and research strategy is proposed to gain insight into perceptions and decisions as to how SMBs make decisions regarding cybersecurity hygiene measures, which could lead to better-informed decisions regarding insurance as part of an ISA program, as well as have a bearing on policy structures and pricing for such insurance. This is because the definition of "cybersecurity hygiene habits"(CHH) as a task appears to vary within the industry and makes the practice hard to measure and evaluate. Research suggests that there may be a poorly understood connection between CHHs undertaken by organizations and their perceptions and/or adoption of cybersecurity insurance as well, thus leading to gaps or holes within business security perimeters. Homeostatic Risk Theory (HRT) has been observed in other venues in which the use of risk mitigation measures (including insurance) leads to more risky behavior; this may have a bearing on why so many organizations, particularly Small and Medium Businesses (SMBs) are very slow to adopt Information Security Assurance (ISA) measures at all or do so minimally. This paper presents a theoretical framework and proposed research, which will provide greater clarity on these issues while highlighting areas where further research is required.

Keywords: Cyber Hygiene, Cyber Insurance, Information Security Assurance, Homeostasis

Cyber insurance effects on cyber hygiene: Does the Homeostatic Effect apply?

Borrowing from the work of the famous physicist and philosopher, Thomas Kuhn, who coined the term paradigm shift, the purpose of this paper is to explore the possibility of a homeostatic shift creeping into this twenty-first-century field of Information Security Assurance (ISA) as it relates to risk management and mitigation. Since there is limited information and research to address this topic, we believe this topic needs to be further explored. Specifically, the over-arching purpose of this paper is to present the case to investigate the question *How are Cyber Hygiene Habits (CHH), which are seen as protective controls used within the overall Risk Management (RM) process, modified, changed, or impacted after Cyber Risk Insurance (CRI) is purchased or simply modified due to Risk Homeostasis Theory (RHT)*, explained later in this paper.

In a phased-research investigation, researchers present the elements of theory within this paper to set the stage for a larger data collection project planned for the fall of 2021, Phase 2 if you will, in which data collected will be discussed as it applies to changing CHH whether through RHT, cultural conditions or even from a confusion of the term or hygiene tasks themselves. Therefore, while the authors do not intend to imply there is a relationship between these elements between lessened habits or even that RHT exists in the cyber realm, this manuscript explores the theoretical possibility and the need to examine the

relationship and review evaluation measures (tools) between that of insurance confidence and cyber hygiene diligence in which RHT may play a role.

Lastly, utilizing a newly created SAFETY CHH inventory tool constructed using an agreed-upon definition for CHH-related tasks, RHT will be used as a framework to examine contributing factors that may lead to lacking or detrimentally modified habits for cyber hygiene. When modified or reduced, errant habits allow for more prevalent, and possibly larger, data breaches to be seen well into the future. Data is expected to be collected using a convenience sample from past and current CHH personnel as the authors ask how Small-to-Medium Businesses (SMB) are managing data hygiene practices. They will be asked, once CRI is purchased, and to what degree was/is there a reduction in CHH based upon basic insurance policyholder assumptions after CRI is purchased.

Through this lens, the following more-defined research questions have emerged and will be investigated individually as they apply to each phase of this project. However, only the theoretical aspects behind the creation of these questions will be addressed during this initial phase and paper to best frame our research goals and to discuss the new inventory tool's construction. The research questions are as follows:

Research Question 1 (RQ1): Does cyber insurance alter cyber hygiene behavior?
*(*Phase 2 Fall of 2021*)*
Research Question 2 (RQ2): What role does cyber hygiene play on insurability? (Phase 2)
Research Question 3 (RQ3): What role does cyber hygiene play in claims denial? (Phase2/3)

However, it should be noted that RQ1 is the primary concern during the initial phases of this study as it is vitally important as more and more organizations consider both cyber insurance and their cyber risk profile and associated hygiene. Thus, a theoretical approach is the nature of this paper to set the stage for a larger investigation.

Literature review

Definition of Cyber Hygiene Habits (CHH)

Within the information systems security and assurance field, there is a lack of consensus on a unified cyber hygiene definition. It should be noted that literature regarding this topic is very limited due to this confusion found in the field. Therefore, this literature review is meant to set a theoretical lens in which to set the stage for a larger investigation. This is the larger issue that has emerged in the field as recently as 2020. Vishwanath et al. (2020) state,

> While many experts lament the lack of cyber hygiene, it's unclear what cyber hygiene really means […and] adding to the confusion, a search on Google's search engine returns hundreds of web pages authored by bloggers, IT companies, and different shades of cybersecurity experts espousing all manner of suggestions from the obvious […] to the highly specific, (p. 1).

Thus, for the sake of this study, the authors are making Homeostasis measurement a secondary condition rather than a theoretical application due to varying CHH field definitions. However, we must first examine habits that differentiate between those who have purchased insurance in comparison to those of the cyber uninsured, and the need for additional phases and continued data dissemination must continue in steps.

Usually when one thinks of insurance, one thinks of auto, health, or even home insurance policies. While there is debate regarding when the first cyber insurance policy was written (and by what underwriter), the marketplace of coverage options has expanded significantly over the last twenty years. By 2009, the concept was becoming engrained in foundational-level college textbooks for information security (Whitman, 2009). Over the last two to three decades, the literature on risk management in general and cybersecurity risk mitigation, in particular, have also helped establish the use of insurance as a risk-sharing strategy, in which the use of insurance to share risk has become a mainstay topic. However, this is a view that is often presented with little critical examination. It's as if cybersecurity experts or information security managers are not expected to make or influence decisions regarding coverage and policy specifics -- at least until a claim needs to be attempted. Mostly this association grew out of the need for a method to secure data or recover damages caused by the multitude of data breaches on a global scale. With this automaticity of thought, general protections may be assumed regarding the purchasing of CRI policies. These policies differ greatly from the general insurance industry and even within the ISA field itself, a field in which the definition of cyber hygiene is not properly defined, much less any consistent agreement on what constitutes an accepted minimum set of such hygiene habits to practice.

The phrase "Cyber Hygiene Habits (CHH)" does show up quite frequently as part of consumer-oriented advice on the web pages and blogs of companies offering retail information security products and services. It's also appearing with greater frequency on web pages of consulting and security services providers, aiming to engage potential business and government customers. Across these various pages are offered nine or more steps (Brook, 2020; Norton, 2021; RSI Security, 2021) as the recommended daily routine activities to achieve better cybersecurity by habituating these as part of one's routine.

This gives a clearer place to start from: first, identify what constitutes a working definition of cyber hygiene, with that as a foundation, then identify a set of habits to ingrain into organizational business processes and practices. Government agencies in multiple countries, from Australia through the United States, offer both nontechnical and technical advice to SMBs and others as to what features to implement in a cyber hygiene program. One of the most widely recognized frameworks for this guidance comes from the Center for Information Security (CIS) (n.d.), which has organized its most urgently recommended controls into what it calls implementation groups. Implementation Group 1, for example, is expressly positioned for organizations with little technical or operational cybersecurity knowledge and experience. It stands to reason that these types of organizations are quite possibly the most at risk of significantly underestimating the risks to their businesses from cyberattacks, especially ransomware attacks and that they could benefit the most from an insurance coverage package that is supported with underwriter recommendations for better security measures that could lead to reduced premiums or more complete coverage of loss.

CIS' Implementation Groups 2 and 3 layer on more powerful, sophisticated security control processes, which in many cases are levied as compliance mandates via law, regulation, or contracts upon more sophisticated enterprises. These organizations generally should be expected to have the in-house technical, operational, and financial expertise necessary to use insurance effectively as part of their information security assurance programs. It's not clear, however, that sufficiently sophisticated insurance vehicles exist to serve these organizations.

In many other aspects of business activities, the legal concept of the *reasonable person test* provides an effective way to link the contemplation of alternatives (and hence decisions to be made) to the duties of due care and due diligence. Nourse's (2008) assessment of this test as a decision heuristic, rather than a hypothetical person, is perhaps revealing of the problem at the heart of the CHH decision-making -- or failure to *make* decisions -- processes that many organizations use. Vishwanath et al. (2020) have

commented on "the impact of cyber hygiene on three facets of human cyber interaction [are]: a self-belief about technology use, a critical facet of individual cognitive processing known to impact cyber resilience, and an online behavior that users all over the world regularly engage," (p. 9), which suggests that perhaps the reasonable person heuristic is tuning itself to selectively ignore the gray rhinos (Wucker, 2016) that are the cybersecurity risks.

Risk Homeostasis Theory (RHT)

The purchasing of CRI may cause a false sense of security, known as the Risk Homeostasis Theory (RHT). RHT could cause unforeseen elements or gaps in protection that could cause more damage than expected. This condition needs to be further examined for relationship correlations between CHH and the purchasing of CRI. Thus, field processes and RM control conditions that reside under the CHH heading must first be examined after CRI is purchased as its application introduces a change in the perceived closed-loop cycle of RM and identification causing levels of acceptable risk to rise or fall depending upon how the purchasing of CRI is viewed. Due to the gravity of a change of this nature, some may compare this condition to that of the rise and fall of the dot-com era, one of the largest paradigm shifts witnessed within the most recent decades.

The concept of Wilde's (1982) RHT can be distilled down to the notion that the more actual or perceived protections against a risk one has, the more risk one is willing to accept since protection offsets risk allowing one to maintain the same risk tolerance yet engage in more risky behavior. This phenomenon has been observed in aviation, general safety science, and any place risk is present. Pless (2016) effectively summarizes numerous RHT studies citing the Munich Taxi study where half of the cabs were equipped with Anti-Lock Brakes (ABS) and the other half were not. The accident rates were effectively the same because those with ABS drove more aggressively in inclement weather negating the safety benefit by increasing the risk (Homeostasis). The same pattern was observed when high-end cars were first equipped with airbags and the accident rate increased in a counterintuitive way. Another set of studies reviewed helmet-on versus helmet-off behavior on bicycles and motorcycles. The protective value of the helmet was negated when riders rode more aggressively.

This same phenomenon was observed by Jardine (2020) as it related to commercial antivirus software creating a false sense of security and causing users to increase their risk profile negating some or all of the benefits of the software. RHT when applied to cyber hygiene and cyber risk posits that the more cyber risk protection one has, the more likely one is to increase their overall risk footprint.

The aforementioned mitigations generated the most adverse effect to overall risk when the mitigation was not widely adopted, accepted, or considered new or novel. In practice, now that airbags are in every automobile, the presence of an airbag is less likely to alter driving behavior since that risk mitigation strategy has been normalized and is no longer out of the ordinary. This concept may apply to the cyber protective realm as well. RHT, therefore, suggests that the installation of a risk mitigation strategy may make one engage in more risk-based on risk tolerance as opposed to enjoying the benefits of the mitigation strategy.

Cyber risk insurance and the homeostatic relationship

When thinking of protecting corporate and even personal data where or when are these limits imposed or even best defined, especially if data is not always kept within a person's possession or stored on a local corporate server farm. With the rise of cloud computing, much of the data is stored overseas, sometimes

in the same location as the actor (attacker) themselves. Still, the term insurance might provide a false sense of security, and corporations who have purchased insurance may continue to conduct "business as usual."

In the insurance realm, there are policy coverage limits, deductibles, and premiums. For obvious reasons, insurance is greatly different than performing cybersecurity tasks – those falling under the CHH umbrella, and usually this understanding is not up for debate amongst practitioners and educators alike. However, assumptions within the field regarding insurance may cause some who are less familiar with the cyber insurance industry and practices, or those who conduct business within an SMB market, to simply equate the two risk treatment choices - transfer or mitigate - as equal.

Yet, for those who have purchased insurance and attempt to make a claim against their policy due to a data breach, many claims are being only partially paid or outright rejected (Kshetri, 2020) since the data breach is considered an act of terrorism due to the origin of the attack. Many policyholders are only made aware of this outcome at that very moment of claim and soon realize the harsh reality of the real need to be knowledgeable of the small print. Business owners then turn to the courts for resolution only to find out they too need to be more diligent in their cyber hygiene efforts and are held further accountable by the court system in which they sought justice. Thus, the court's find in favor of the insurance companies and uphold the decision to reject the claim and lost are the additional working hours, court and lawyer fees, and the original data taken or made corrupt by the breach itself.

CRI may or may not be a solution to offer protection from cybercrime fallout at any level. If homeostasis does exist and the effects are not accounted for within a policy or risk assessment benchmark collection, the policy may be void since the contract is unable to provide coverage for the unknown change in risk acceptance level. Further, if the concept of protection is lost by the sheer notion of this theory's concept that risk level can be changed by a new denominator and the results of the change outcome may be subjective (Wilde, 1998) and not predictable, thus, this is seen as reflexive.

RHT showcases the lack of the continuation of true protection when up against unknown actions on the part of the administrators and staff operating within any area of the ISA collaborative departments. However, we must ask what are these actions in the true sense of the word – report reviewing, employee training, or other? What is taking place when a safety net, such as CRI, is implemented – does IT become less reactive to security events as they believe the corporation is safer and always protected, or do they become overly cautious and restrict the overall business processes that ISA seeks to protect?

Methodology

With so many in disagreement about the definition of cyber hygiene (Vishwanath et al., 2020), to poll for CHH terms and tasks, the previous authors utilized a process known as Concept Mapping to gather data but utilized a limited sample that now needs to be expanded. Originally utilizing a Confirmatory Factor Analysis (CFA), the researchers created a Cyber Hygiene Inventory (CHI) instrument to support future field measurements of CHH and practices. During CHI survey instrument creation, a SAFETY inventory was realized, one that comprised of five categories. Validation results of the CHI tool were tabulated and ranged from alpha reliability 0.75 to 0.89 within each of these five categories. Through validation five cyber hygiene dimensions were identified alongside validation results creating the SAFETY acronym: (a) [S] Storage and device ($\alpha = .86$), (b) Authentication and credential ($\alpha = .84$), (c) Facebook and social media ($\alpha = .89$), (d) Email and messaging ($\alpha = .84$), and (e) Transmission and browsing ($\alpha = .75$). This tool will be used to gather data in the fall of 2021, Phase 2.

With permission from the original survey authors in personal correspondence, the current research intends to extend this survey tool to allow for a larger examination for correlations between the purchasing of CRI to that of changes in CHH due to RHT and possibly COVID-19 habits but will support external validation efforts and help to solidify an industry-accepted cyber hygiene definition based upon the SAFETY framework. The modified survey instrument includes survey questions that inquire about the corporate size, the selection to purchase cyber insurance, and questions to ascertain if CHH have changed after purchasing insurance if applicable.

Through this extended survey process, it is expected that data will shine light upon the variance within these terms, processes, and further extend the investigation of a unified CHH definition, but to also allow the researchers of this current project to truly examine for changes that may support the following hypothesis:

> H0: There is no significant difference in Cyber Hygiene Habits (CHH) between those who purchase Cyber Risk Insurance (CRI) in comparison to those who have not.
> H1: There is a significant difference in Cyber Hygiene Habits (CHH) between those who purchase Cyber Risk Insurance (CRI) in comparison to those who have not.
>
> H0: There is no significant difference in the definition and identification of Cyber Hygiene Habits (CHH) between those who purchase Cyber Risk Insurance (CRI) in comparison to those who have not.
> H1: There is no significant difference in the definition and identification of Cyber Hygiene Habits (CHH) between those who purchase Cyber Risk Insurance (CRI) in comparison to those who have not.

Homeostasis effects may present themselves during analysis as the authors seek to understand if simply possessing cyber insurance alters cyber hygiene behaviors but will only be further investigated should the data present a strong correlation. Similar to automobile insurance where coverage and rates are based on drive profile, there does not appear to be a profile that insurance companies use from which to identify risk or even understand premiums in the cyber realm as of yet. Nor do these premiums provide incentives for those upholding better practices.

Once the extended survey items are combined with the original SAFETY framework, this tool will provide our industry with a unified measurement tool and powerful data allowing for greater triangulation for those that examine common hygiene tasks and practices for greater risk management and support. This inventory tool could be a powerful instrument to be used widely within the industry since no such tool has existed prior. If utilizing this tool, the results found in future investigations would no longer be ambiguous across domains and varying business operating conditions. Thus, helping to extend the overall body and field knowledge. This phase intends to share the theory and creation behind this updated tool.

Future research plans

Similar to both Jardine's (2020) and Pless's (2016) examples, the authors posit CRI should be viewed as a risk mitigation strategy for organizations as presented in Figure 1 – The Relationship between Cyber Hygiene Habits (CHH) and Cyber Insurance. This research that will be conducted in later phases of this project attempt to hypothesize the possible gaps by organizing these gaps into three categories for future exploration. These "gaps" are referenced in Figure 1 as well. These gaps are based upon the understanding of Risk Homeostasis (RH) and Kuhn's paradigm theory as the thought lens in which to examine potential fallout if Homeostasis is found to affect the cybersecurity landscape of a corporation.

Through the suggestion of a theoretical model, as diagrammed by using a 2X2 matrix, the investigative design seeks to confirm identified gaps in the risk management framework.

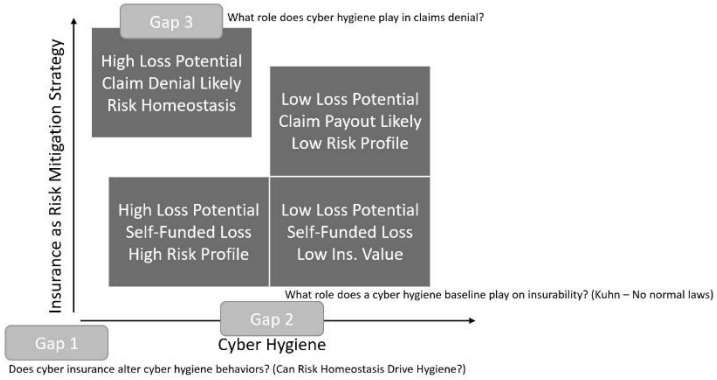

Figure 1: The Relationship between Cyber Hygiene Habits (CHH) and Cyber Insurance

Thus, additional phases of the project will be added as needed based upon future findings, and will focus upon the following Research Questions:

> *Research Question 2 (RQ2): What role does cyber hygiene play on insurability?*
> *Research Question 3 (RQ3): What role does cyber hygiene play in claims denial?*

RQ2 seeks to understand how insurance companies and hygiene expectations for insurability are in the pre-parading phase using Kuhn's theory with the notion of *we lack normal laws and there is no consensus is present*. RQ3 attempts to practically apply these concepts to move the field towards normal laws, a paradigm shift of sorts. Understanding claim denials as a function of cyber hygiene will help better define cyber hygiene, insurability, and enable organizations to benefit from cyber insurance and for cyber insurance companies to better understand their own risk calculations.

References

Brook, C. (2020, Oct 6). A definition of cyber hygiene, benefits, best practices, and more [blog]. https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more

Center for Internet Security. (n.d.) V7.1 introduces implementation groups to the CIS Controls ™). https://www.cisecurity.org/blog/v7-1-introduces-implementation-groups-cis-controls/

Jardine, E. (2020). The case against commercial antivirus software: Risk homeostasis and information problems in cybersecurity. Risk Analysis, 40(8), 1571-1588. https://doi.org/10.1111/risa.13534

Kshetri, N. (2020). The evolution of cyber-insurance industry and market: An institutional analysis. Telecommunications Policy, 44. https://doi.org/10.1016/j.telpol.2020.102007

Norton. (2021, Jan 23). Good cyber hygiene habits to help stay safe online. https://us.norton.com/internetsecurity-how-to-good-cyber-hygiene.html

Nourse, V. (2008). After the reasonable man: Getting over the subjectivity / objectivity question. Georgetown Law Library Commons

Pless, B. (2016). Risk compensation: Revisited and rebutted. Safety, 2(3) doi:http://dx.doi.org.ezproxy.libproxy.db.erau.edu/10.3390/safety203001

RSI Security. (2021). The top 11 rules of cyber hygiene for government agencies. https://blog.rsisecurity.com/the-top-11-rules-of-cyber-hygiene-for-government-agencies/

Vishwanath, A., Neo, L. S., Goh, PW., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. Decision Support Systems, 128. https://doi.org/10.1016/j.dss.2019.113160

Whitman, M.E., & Mattord, H. J. (2009). Principles of Information Security (3rd ed.). Course Technology / Cengage

Wilde, G. J. (1982). The theory of Risk Homeostasis: Implications for safety and health. Risk Analysis, 2(4), 209–225. https://doi.org/10.1111/j.1539-6924.1982.tb01384.x

Wilde, G. J. S. (1998). Risk homeostasis theory: an overview. Injury Preventions, 4, 89-91

Wucker, M. (2016). The gray rhino: How to recognize and act on the obvious dangers we ignore. St Martin's Press