White Paper
December 2019

Stop saying "Cyber Hygiene is like personal hygiene"

Arun Vishwanath, PhD, MBA; Technologist and CTO, Avant Research Group, LLC;
Website: *https://arunvishwanath.us;* Email: *arun@arunvishwanath.us*

Keywords: cyber hygiene, science of cyber security, human factors, OPSEC

"Users should use a range of letters, numbers, and special characters on their passwords and change it every 90 days." If you are in IT, you have likely implemented this security policy. And if you are a user, you have likely endured it.

The source of this best practice suggestion is a Burr, Dodson, and Polk (2004)[i] NIST publication, which Microsoft and others widely publicized and implemented[ii]. Only, this practice has many critical flaws: it forces users to come-up with difficult passwords, often, so they end up reusing passwords across services; and it makes password reset emails common—so when a phishing email comes in asking to reset a password, users are far more likely to comply. Recognizing this, NIST reversed the policy in 2017, but by then, IT managers all over the world had blindly followed the best practice for more than a decade.

Cyber hygiene practice suggestions such as this, however, do not end here. There are many more. At the broad end are suggestions such as "develop a process for software installation for end users" or the ever relevant "educate your users on good cyber behavior." While at the specific end are ideas such as "always use a VPN when connecting to networks," "always look for SSL (lock) icons on webpages," "always look for source headers in emails to find out who is sending you an email," "always use a password vault," "always use a good virus protection programs," and "always apply patches and keep your system software updated." All follow a familiar pattern albeit with varying levels of specificity: they expect the user to blindly perform an action, all the time, when online.

But are these blanket suggestions really appropriate? Are they even effective, let alone necessary to do in all cases, across all organizations, by every Internet user around the world?

Answering such questions might appear unnecessary, but there is a cost involved in asking computer users to check various parts of an email's header for each email they receive, to use a VPN, or to manage their passwords in vaults. The costs are not just in their time but also in the technical IT resources that go into supporting such practices, not to mention the aforementioned issues of users becoming habituated in flawed practices, which could increase their vulnerability to cyber compromise.

Whenever such criticisms are raised, cyber security experts resort to conceptual analogies, drawing parallels between cyber hygiene best practices and personal

hygiene, to justify their suggestions. The usual argument is along the lines of "just like washing hands, brushing teeth, or regularly taking multivitamins," “users should do this…” and besides “just like personal hygiene, there is also no real harm in following cyber hygiene best practice guidelines.”

But if we have learnt anything from research on public health, it is that not all suggestions are good. This is the lesson from the widespread intake of multi-vitamin pills as well. While most people believe vitamins are necessary or that there is no harm in taking them, medical research disagrees. After reviewing multiple large-scale tracking studies, the medical community concluded that vitamins have little to no effect whatsoever on reducing heart disease, cancer, cognitive decline, or memory loss. In fact, some, such as vitamin E and beta-carotene supplements, are downright harmful and reduce life expectancy instead of improving life.[iii]

Of course, there are exceptional times where vitamins are good or even necessary. Certain people—pregnant women, people living in certain regions, people suffering certain health ailments—might need a course of vitamins.[iv] These conclusions are supported by research and are based on a case-by-case assessment of the person’s needs.

The same is true for cyber hygiene best practices. Not all work, but some do. But what works, and the specific instances—organizational type, use environments, use cases, and user types—need to be ascertained. These need to be empirically determined and evaluated for their need and contextual adequacy. Doing so is far better than blindly implementing hygiene practices on the advice of sundry sources, without assessing their applicability, only to realize years later that it was not only a wasted effort but that it also made the organization more vulnerable to cyber-attacks.

The paper presents a better approach. It begins by examining the basic concept of cyber hygiene, a term that is widely used but poorly understood or conceptualized. Next, the paper tracks the roots of the concept of cyber hygiene and discusses the pitfalls of comparing it to personal hygiene. Following this, the paper presents a recently developed measurement tool called the Cyber Hygiene Inventory (CHI) and discusses how it can serve as a framework for developing need based cyber hygiene practices.

What is cyber hygiene?

In early 2015, in the aftermath of the Sony Pictures Entertainment hack, while writing a media article on how we can prevent cyber breaches, I was searching for a term that captured what online users could do to better protect organizations from such attacks. My search led me to a 2013 Wilson Center speech by then Homeland Security Secretary Janet Napolitano who had used the term "cyber hygiene" in the context of cyber habits. [v] I thought the term was perfect because it helped drive home the message that protecting the Internet was every user’s personal responsibility. I used the term in my article[vi] and in many others, with one local newscaster during an interview even commenting on the term’s simplicity and catchiness.

Thanks to its appeal, today the term is so common that a keyword search on Google returns over 33 million pages with the phrase cyber hygiene. It has appeared in public policy documents, military doctrines, congressional testimonies, media articles, research papers, and websites. All subscribe to some definition of what cyber hygiene

entails and espouse all manner of best practice guidelines. Some of these guidelines target adolescents, others are for employees, some others focus on IT professionals, and still others on vulnerable populations.

But while there are many suggestions on what constitutes cyber hygiene, there is little clarity on what it does or does not entail and who it should be performed by. This is a problem across the globe. In comparing cyber hygiene practices across member nations, the European Union Agency for Network and Information Security (ENISA) found that there was no single standard or commonly agreed upon approach to it. The report also concluded that cyber hygiene should be viewed in the same manner as personal hygiene in order to ensure the organization's health was in optimum condition. (ENISA December 2016). (https://www.enisa.europa.eu/publications/cyber-hygiene/at_download/fullReport). Thus, there is no clarity on what cyber hygiene means or entails other than the view that it is something akin to personal hygiene. But while it's unarguable that cyber hygiene is important, is it really appropriate to think of it in terms of personal hygiene?

Is Cyber Hygiene Analogous to Personal Hygiene?

The metaphorical construction of cyber hygiene as similar to personal hygiene does not stop at its definition. It even influences how cyber safety solutions are framed. For instance, many cyber security websites use examples of hand washing and multivitamin used to drive home cyber safety suggestions, such as applying virus updates and patches. Some sites go even further. One in particular, "Cyber Security is Cyber Health"[vii] equates poor heredity in people to the use of obsolete software; the lack of vaccinations to the lack of technical safeguards; and promiscuous sex with visits to unreliable websites. It makes similar conceptual leaps linking pregnancy, fetal ultrasound, newborns, even psychological health, with some sundry facet of cyber hygiene.

Thinking in this manner adversely influences the solutions we develop. Take the case of airplane technology. Since antiquity our mental models of flying were based on avian flight because the flying capabilities of birds were visible and self-evident. From the ancient Greek fables of Daedalus and Icarus mythologizing the use of bird-like wings for human flight to 20th century attempts at fabricating aircraft's wings that flapped, this analogous thinking stymied the development of aircraft technology for over two millennia. Figure 1 is the 1857 patent drawing of pioneering aviator Jean Marie Le Bris's failed Artificial Albatross.[viii] It shows how the avian model proved to be a proverbial albatross in aircraft design. Thus, the analogies we use for thinking about cyber hygiene matter.

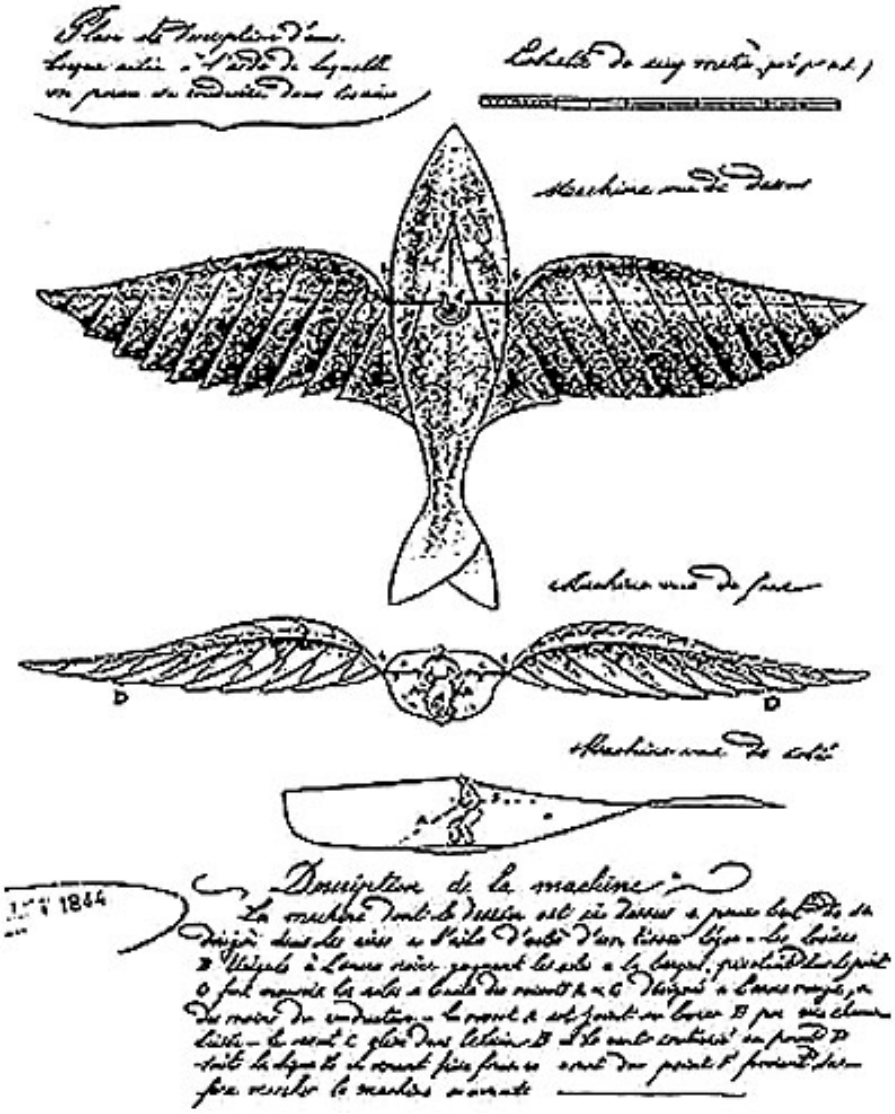

Figure 1. Patent drawing of pioneering aviator Jean Marie Le Bris's Artificial Albatross

There is another reason for unbridling cyber hygiene from our mental models of personal hygiene. Personal hygiene does not have a downside. Washing hands or brushing teeth, unless you do it at an obsessive level, does not cause problems to people. But using a certain app or an operating system thinking it is protective could enhance risk, especially if we trust such systems. For instance, telling people to believe that "an SSL website is secure" is just bad policy not only because many fraudulent websites also have legitimate SSL certificates but also because users conflate security with safety, wrongly thinking secure sites are authentic sites.[ix] Making such wrongful thinking even more problematic is the fact that more and more phishing websites—two out of three according to a recent Anti Phishing Working Group (APWG) report—have SSL certificates.[x] Users need not compulsively enact behaviors based on such flawed beliefs. All it takes is for them to enter their credentials on what they purport is an encrypted page on one of these phishing websites for a breach to occur.

The same problem plagues us if we place too much credence in a solution, again, something we do not really think about in our physical hygiene. Believing that a virus protection solution is protective or that all its updates that appear as notifications are necessary, making users blindly apply patches. Unfortunately, many social engineering attacks mimic software and virus protection updates, which users wittingly download and apply because they have been conditioned to behave as such. In this way, cyber hygiene practices can make users more rather than less vulnerable.

But there is yet another important difference between the personal and cyber realms stemming from what they protect. Personal hygiene protects the human body from chance infections through routine preventative actions. The human body is, however, already resilient. Even without many modern hygiene solutions such as hand soap, humans can ward off many threats. The central reason for this is defenses against most germs and viruses we have evolved over millennia. Our sensory organs have evolved follicles, hair, nails, eyelashes, cilia, and mucous membranes that trap most intrusion. Our internal organs likewise have also evolved complex immune responses that work independently of our need to manage or control it. These internal and external defenses work in tandem and independently when needed and are further protected by the human brain (such as when someone impulsively swats a stinging bug). Thanks to these complex systems, most of us can live relatively long disease-free lives with minimal need for modern medicine.

In contrast, while technology is collectively capable of highly sophisticated computational tasks, its core components are dumb circuits that built without any effective protection and often flawed at their very core. Take computer processing chips and memory cells, the computer's internal organs, for example. Last year, the identification of Meltdown and Spectre vulnerabilities demonstrated that nearly every computer chip manufactured in the past two decades have critical flaws in their algorithmic structures, rendering them vulnerable to various exploits. Similarly, dynamic memory cells or D-RAMs are also vulnerable to leaking their electrical charges as they interact—called the rowhammer effect[xi]—which can be exploited in a D-RAM attack to get root access to systems.

The same is the case for the "sensory organs" of computing devices: touchpads, microphones, cameras, and input devices. Each is easily corruptible using simple keyloggers and other programs. Layered on these are many apps, all using different schemes and privileges that interface with the system's internal organs. Some of these apps are programmed poorly, others are rouge programs built to affect compromises by co-opting their privileges, while still others can be manipulated by rouge programmers using malware that can infect everything from the sensory organs of the computer all to way to its internals. Finally, we have users with varying skills who utilize these systems and programs on them in a multitude of ways.

Making things particularly different, a single computing attack can cripple multiple layers of computing without needing to evolve a compromise for each layer. As a case in point, a single phishing email with a malware payload can trick users, circumvent many end-point security protections, and enter the core of a system and gain a foothold. In contrast, even influenza, one of the most lethal and persistent biological viruses,

which kills over 600,000 people globally each year, requires a complex series of interactions. Over two-thirds of deaths from it are because of indirect causes such as organ failure.[xii]

Thanks to all this, human hygiene practices can accommodate a wide amount of variance in outcomes. In contrast, errors in individual cyber hygiene practices can have a geometric increase in overall risk because the system risks exponentially heighten at every iteration. For instance, a 10 percent failure rate in hand-washing rates does little to increase infection from most diseases. In contrast, a 10 percent failure rate in SSL certificates could lead to enhanced risk by itself. If these certificates are used in email-based phishing attacks with a 10 percent relevance rate (users for whom the content is relevant), on an email network that allowed 10 percent of these emails through, with just 10 percent of the users clicking and enabling the malware, the probability of a breach goes up to 34 percent.[1] These are conservative probabilities because in actuality 30 to 70 percent of phishing emails are usually opened (Caputo et al. 2013)[xiii] and there are many rouge SSL certificates and pages on the Internet.[xiv] Thus, each potential failure magnifies the overall failure rate, something which seldom occurs in human beings because of the way evolution has helped us defend ourselves.

What is clear from this is that hygiene in health and cyber hygiene are not analogous. Differences stem from the nature of computing, online threats, and users—all of which cumulatively increase the risk of a breach. Because of this, we cannot afford the same leeway with cyber hygiene that we can with personal hygiene. We need greater precision in how we define cyber hygiene and identify policies.

So what is user cyber hygiene?

Until recently, there have been few academic attempts at defining cyber hygiene. By comparing various definitions, through interviews with IT personnel, CSOs, CIOs, and using a quantitative scale development approach, Vishwanath et al. (2019) developed a conceptual definition and a multi-item inventory for measuring cyber hygiene. They define cyber hygiene as the cyber security practices that online consumers should engage in to protect the safety and integrity of their personal information on their Internet enabled devices from being compromised in a cyber-attack (Vishwanath et al. 2019).[xv]

At the operational or measurement end, user cyber hygiene comes from the confluence of four user-centric factors: awareness, knowledge, technical capacity, and the enactment of cyber security practices. Awareness and knowledge make up the cognitive factors of familiarity and understanding. Technical capacity pertains to the availability of technologies where necessary. Finally, enactment makes up the behavioral dimension and is the utilization factor. Effective user cyber hygiene occurs at the confluence of these four factors: when users, aware of what needs to be done, are knowledgeable about it, have the required technologies and know-how to achieve it, and enact it as and when necessary.

Vishwanath et al. (2019) also developed a framework that can be applied across multiple organizational and user environments. It is organized using a multi-dimensional inventory called the Cyber Hygiene Inventory (CHI).[xvi] The CHI comprises 20-items or

[1] The dependent probability is computed as (1-.90^*k*), where *k* is the number of layers of vulnerability.

questions that tap into five dimensions of user cyber hygiene. These dimensions are organized using the acronym SAFETY, where S pertains to Storage and Device hygiene, A signifies Authentication and Credential hygiene, F signifies Facebook and Social Media hygiene, E pertains to Email and Messaging, T for Transmission hygiene, and Y stands for "you" signifying the users responsibility in ensuring cyber hygiene. Each item or question in the inventory measures a best practice or a cyber safety related thought or action. While the inventory has a finite set of 20-items, it allows for the addition of questions that are often necessary to capture contextual or organization-specific practices.

Before delving into the details of the inventory, some facets of the inventory need highlighting. First, the framework provided by CHI is broad and technology agnostic. This has two advantages: it allows the CHI to be applied across any organization, user group, and even residents of an area. Second, having a broad inventory makes it possible to use it across platforms, technologies, applications, over different points of time even as different platforms and functionalities evolve. Third, we can measure most questions in the CHI using standard survey approaches. Fourth, the CHI accommodates subjective and objective measurements. While knowledge, capacity, and behavioral intent, can all be measured subjectively, we can also measure them using objective measures using a knowledge test, by taking an inventory of technologies available in the organization, and by measuring actual behavior observationally. Using a combination of measurement approaches has the added advantage of eliminating confounds such as method bias from influencing the results. Finally, the CHI includes measures of cognitive and behavioral factors. This is superior to extant approaches such as using pen-testing data or training data, which only capture behavior. Thus, the CHI captures information about user related to their cyber hygiene with more granularity, accounts for more user-level influences, and allows for more valid measurement of users' cyber safety related thoughts and behaviors.

In the ideal case, the CHI can be used to evaluate all 4 aspects of cyber hygiene—awareness, knowledge, capacity, and enactment—using a 0-5 scale. This gives each dimension a range of responses from 0 to 100, making it possible to derive a cumulative score that is easily interpretable and comparable across the inventory's implementations. Thus, at a minimum, the score can compare awareness against knowledge, know-how, and intent among users within an organization. Using the score comes with all the usual caveats: the score is inherently ordinal but being treated as a ratio; technical know-how is contingent on IT supplying them; the responses on some enactment frequency questions are limited by the technology, application, and platform. Most of these are familiar to anyone trained in empirical social science research, and can be handled through design and analysis.

Thus, the CHI provides a baseline for IT managers not just for understanding users but also for strategic decisions. Often, IT managers hoping to implement various hygiene solutions need to determine their relative impacts and merits. In such instances, the CHI can help ascertain the strategic merits of the intervention and the values different technological solutions they plan to implement. Figure 2 provides an exemplar where 20 items were added to the CHI's 20 and the overall 40 items were

scored on 2-dimensions: their utility or security impact and the perceive ease of using the technology, two fundamental dimensions that information systems models such as the Technology Acceptance Model (Davis et al., 1989)[xvii] have shown to predict the adoption and use of technology within organizations.

Responses by a sample of IT managers within an organization were used to develop the two-dimensional map in the figure. The map presents the overall data in four dimensions, arrayed based on the utility and ease of use of each hygiene practice. The four quadrants in the map are High security significance/utility, Low enactment difficulty; Low security significance/utility, Low enactment difficulty; Low security significance/utility, High enactment difficulty; and High security significance/utility, High enactment difficulty. Based on the map, IT managers can not only quantify the perceptual importance of each cyber hygiene practice and the technology that is most closely associated with it, but also understand the relative effort in terms of resources and expected outcomes from each of them. They can thus, using this approach, strategically choose the cyber hygiene practice and technology they plan to implement.

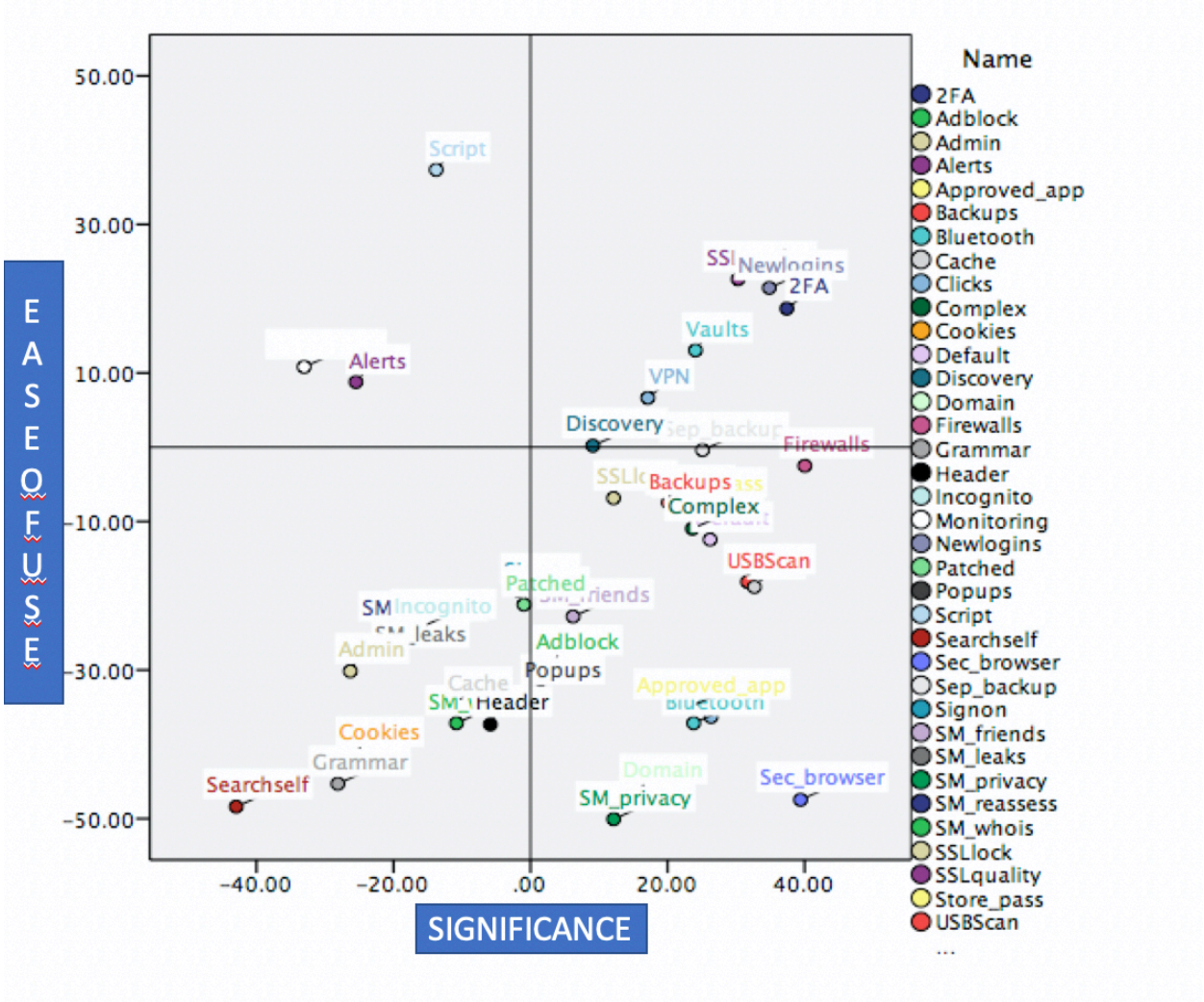

Figure 2. Sample application of the CHI framework to make strategic decisions on organizational cyber hygiene priorities

The CHI can also be used to track the success of individual interventions and improvements in desired levels of cyber hygiene overtime. For this, IT managers can implement the CHI to compare different facets of cyber hygiene—e.g., comparing awareness with utilization at different points in time, such as before and after an intervention; or on different groups, e.g., different divisions of the same organization; or different locations, e.g., one branch of an organization serves as the control while another one in a different location serves as the target. The analysis can focus on charting the individual differences between groups and use the deviation scores or GAPs as a metric of hygiene performance. Figure 3 and 4 provide examples of such implementations. Figure 3 charts data from a single organization's users on their relative levels of awareness, knowledge, and technical capacity across the five SAFETY dimensions of cyber hygiene. Figure 4 tracks the relative impact of training levels on cyber hygiene across users in an organization where the CHI was implemented a month before and after training.

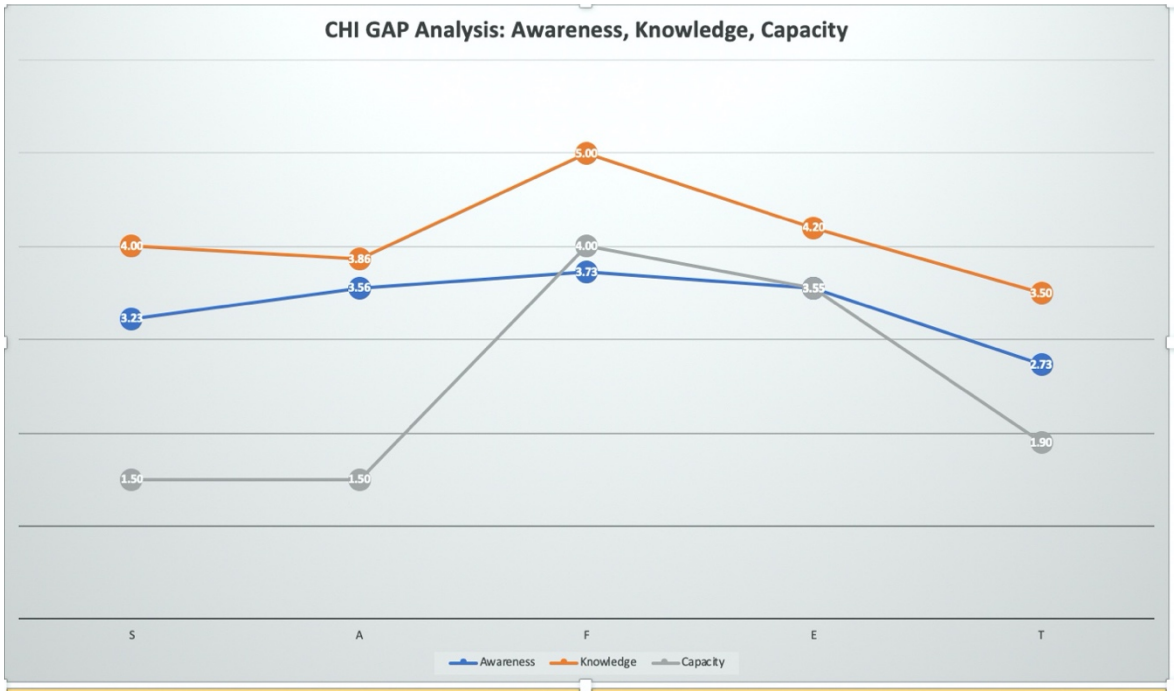

Figure 3. Application of the CHI to assess relative gaps in perceived awareness, knowledge, and capacity

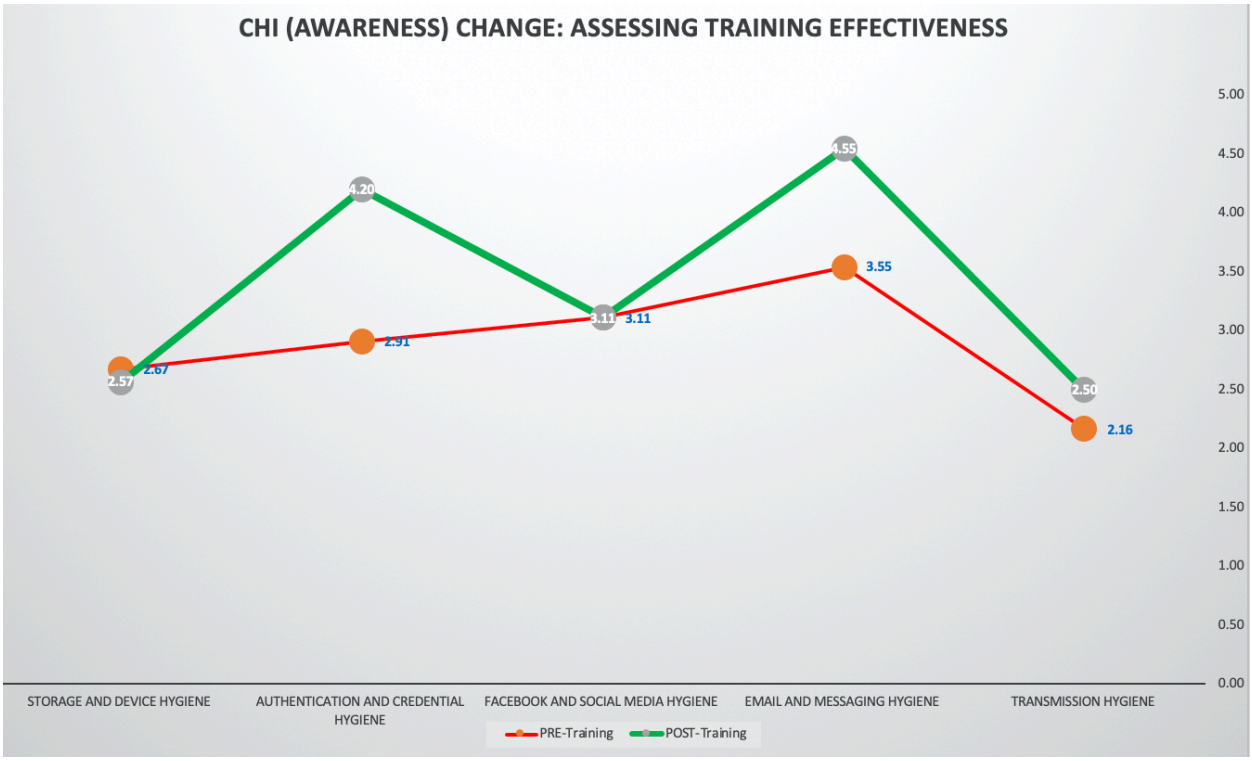

Figure 4. Application of the CHI to assess training effects in an organization.

Advantages of the CHI approach

There is no single metric for cyber hygiene, nor is there any method that can achieve any of what the CHI delivers. The extant approaches to defining cyber hygiene and creating best practices — if organizations even engage in them—remains ad hoc, with most organizations adopting practice suggestions from industry groups and other sources. The CHI serves as a baseline for understanding and developing cyber hygiene practices within organizations. It also helps evaluate, develop, assess, track, and quantify cyber hygiene and ensure improvements over time.

The same is the case with the measurement of hygiene. Most organizations do not even measure user cyber hygiene; others use proprietary approaches with underlying algorithms that remain unknown and difficult for others to use or assess. This is the case with the U.S. Department of Homeland Security's Continuous Diagnostic and Monitoring (CDM) program, which gives participating federal government organizations a cyber risk and hygiene score card. Their reason for the lack of transparency in the program's scoring method is that it would end up in the hands of hackers.

That said, it is safe to say that at the user end, the only metrics that exist come from training and pen-testing. Both approaches, while appropriate, are wholly inadequate. Most use behavioral measures and fail to account for user cognition—wrongly presuming that user behavior is wholly premised on a priori thought. They also have unknown amounts of noise in the data stemming from the variance in the pen-test approaches to the specifics of the tests, its frequency, its reach, and its timing. This makes it impossible to use these metrics to compare different organizations, let alone rely on them to make judgments about an individual organization's level of cyber readiness.

In contrast, the CHI provides a transparent approach, where organizations can use and even share their scores across the 20-items without fearing that it would expose the organization's weaknesses to hackers. They could maintain internal records of additional items—such as specific technological safeguards and other practices—that the organization wishes to not reveal. The quantitative metric can also be used to establish a benchmark that could be improved upon when more data is shared across a sector. With more data from across the industry, industry benchmarks could be established overtime, providing a more robust standard for an organization in a sector. Thus, the CHI provides an empirically driven, widely applicable, transparent, quantitative approach for formulating, benchmarking, and tracking user cyber hygiene within organizations.

Conclusive thoughts

The paper discussed why drawing parallels between personal hygiene and cyber is inappropriate, which might stymie the development of solutions and even increase overall user cyber risk. The paper then offered a different methodology and a mechanism for deriving cyber hygiene practice suggestions, one that is not prescriptive but instead empirically calibrated and contextually relevant. While the phrase cyber hygiene appears to have become part of the cybersecurity lexicon, we can still change how we conceptualize it. In the long run, security experts might even consider moving away from the term, replacing it with others such as Operational Security or "OPSEC,", an area of practice developed by the US military which is more applicable in the security domain and can be applied with resorting to anolgoical leaps. OPSEC begins with the assumption that we are in an adversarial situation—a fact that is true in the domain of cybersecurity—and focuses on prioritizing information and developing approaches to ensure that those pieces of information stay protected. This shifts the focus away from global actions and their analogues in public health to tactical approaches that are grounded in adversarial defense. By re-conceptualizing how we think about cyber security, we can move away from broad practices to specific actions, and from dictating cyber hygiene practices to focus instead on protecting critical information—because after all, that is what the hackers are really after.

---

[i] Burr, W. E., Dodson, D. F., & Polk, W. T. (2004). *Electronic authentication guideline* (NIST Special Publication 800-63 Version 1.0). Gaithersburg: National Institute of Standards and Technology.

[ii] Microsoft. (2016, August 31). *Best practices for enforcing password policies*. Retrieved from https://docs.microsoft.com/en-us/previous-versions/technet-magazine/ff741764(v=msdn.10)?redirectedfrom=MSDN

[iii] Is there really any benefit to multivitamins? (n.d.). *Johns Hopkins Medicine.* Retrieved from

https://www.hopkinsmedicine.org/health/wellness-and-prevention/is-there-really-any-benefit-to-multivitamins

Goodman, B. (2014, February 24). Healthy adults shouldn't take vitamin E, Beta Carotene: Expert panel. *MedicineNet.* Retrieved from https://www.medicinenet.com/script/main/art.asp?articlekey=176905

[iv] Scholl, T. O., & Johnson, W. G. (2000). Folic acid: Influence on the outcome of pregnancy. *The American Journal of Clinical Nutrition*, *71*(5), 1295S-1303S.

[v] Spiering, C. (2013, January 24). Janet Napolitano: Internet users need to practice good 'cyber-hygiene'. *Washington Examiner.* Retrieved from https://www.washingtonexaminer.com/janet-napolitano-internet-users-need-to-practice-good-cyber-hygiene

[vi] Vishwanath, A. (2015, February 24). Before decrying the latest cyberbreach, consider your own cyberhygiene. *The Conversation.* Retrieved from https://theconversation.com/before-decrying-the-latest-cyberbreach-consider-your-own-cyberhygiene-37834

[vii] Cyber security is cyber health. (n.d.). *H-X Tech.* Retrieved from https://h-xtech.com/blog-healthcare-analogy

[viii] Early flying machines. (n.d.). *Wikipedia.* Retrieved from https://en.wikipedia.org/wiki/Early_flying_machines

[ix] Hassold, C. (2017, November 2). Have we conditioned web users to be phished? *PhishLabs.* Retrieved from https://info.phishlabs.com/blog/have-we-conditioned-web-users-to-be-phished

[x] Anti-Phishing Working Group. (2019). *Phishing activity trends report: 3rd Quarter 2019* [PDF document]. Retrieved from https://docs.apwg.org/reports/apwg_trends_report_q3_2019.pdf

[xi] Kim, Y., Daly, R., Kim, J., Fallin, C., Lee, J. H., Lee, D., Wilkerson, C., Lai, K., & Mutlu, O. (2016). Rowhammer: Reliability analysis and security implications. *ArXiV,* arXiv:1603.00747.

[xii] Jabr, F. (2017, December 18). How does the flu actually kill people? *Scientific American.*

Retrieved from https://www.scientificamerican.com/article/how-does-the-flu-actually-kill-people/

[xiii] Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2013). Going spear phishing: Exploring embedded training and awareness. *IEEE Security & Privacy*, *12*(1), 28-38.

[xiv] Vishwanath, A. (2018, September 1). Spear phishing has become even more dangerous. *CNN.* Retrieved from https://www.cnn.com/2018/09/01/opinions/spear-phishing-has-become-even-more-dangerous-opinion-vishwanath/index.html

[xv] Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*, *128*, 113160.

[xvi] Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*, *128*, 113160.

[xvii] Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, *35*(8), 982-1003.