FEATURE

The Human Factor in Information Security

The Weakest Link or the Most Fatigued?

Humans represent a mystery to be deciphered by security/cybersecurity experts because their behaviors, attitudes, beliefs, rituals and decisions (the general characteristics that define a culture) constitute a little-understood universe for executives and their heads of security. Frequently cited in various international research projects and reports is the fact that people are the weakest links in the security chain.[1] Time and again, it is determined that, despite all the technical efforts and security procedures, people are highly likely to expose organizations to vulnerabilities.[2]

The literature available to date on the human factor in security/cybersecurity often refers to raising awareness, training and education—all subjects associated with the "education" of individuals in an effort to protect information. The hope and assumption are that people will comply with the expectations of the organization with respect to the information assets to which they have access.[3]

Jeimy J. Cano M., Ph.D, Ed.D., CFE, CICA
Is an academic and international consultant. He has more than 22 years of experience as an executive, academic and professional in the areas of information security, cybersecurity, digital forensics, digital crime, critical infrastructures and IT auditing.

Similarly, studies confirm that despite the education provided and the sanctions established for behaviors that violate the security procedures and processes designed to safeguard information, the vulnerabilities exacerbated by people still materialize, either due to error, omission or deliberate actions that compromise an organization's sensitive information.[4]

The inevitability of failure as a natural phenomenon in any human pursuit becomes the context that security and control practices must not only accept, but also refuse to resign themselves to a *fait accompli*. Security practitioners know that despite their best efforts, risk scenarios such as unauthorized access, data leaks, unreported change to a text, human error or omissions, among others, will materialize, and that understanding by its nature reveals a schism in business practice where what people actually do is far different from what the organization intends for them to do.[5]

This implies that organizations should be prepared to understand and comprehend, on one hand, the different meanings that coexist in regard to data protection practices on the basis of their everyday experience and, on the other hand, the levels of resistance and resilience of individuals confronted with the challenge of security/cybersecurity in an increasingly hyper-connected world.

Consequently, the aim herein is to contextualize the present-day challenges inherent in the security/cybersecurity education of humans in organizations. Thus, it is necessary to go beyond the weakest-link-in-the-chain discourse and move into the "reliable and resistant factor of the system" discourse, which eclipses the viewpoints and limitations of individuals through its recognition that people's behaviors comprise a network of meaning that is fed as much by correct decisions as by lessons learned, forming part of an ongoing process of learning/unlearning about the inevitability of failure.

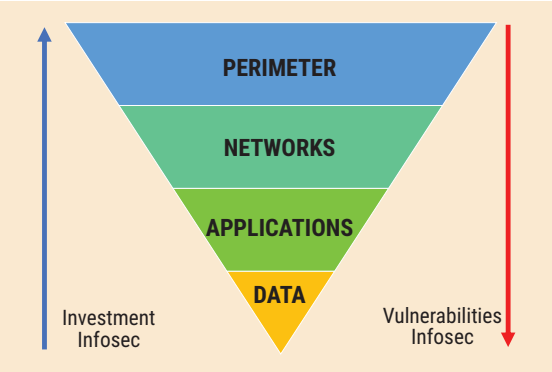
© 2019 ISACA. All rights reserved. *www.isaca.org*

Distribution of Investment in Security/Cybersecurity

Recent reports tell us that investments in security/cybersecurity generally have to do with purchasing and reinforcing infrastructure through new technologies that fine-tune the available capacities of the organization to identify, contain and repel possible attacks or threats designed to compromise information assets.

This reality has not varied substantially since a 2005 study that indicated that the greatest amount of investment in data security was concentrated in perimeter defense infrastructure, while the smallest amount was in data treatment.[6] Subsequent studies based on this 2005 study and using its results show that as investment in the technological periphery grows, vulnerabilities in the area of data treatment are accentuated (**figure 1**).[7, 8] This creates a paradox about where to prioritize and focus efforts to maintain levels of data security within enterprises.

Figure 1—Comparison of Investment and Vulnerabilities in Data Security



In the current context, in which the perimeter is becoming ever more permeable and the digital density around physical objects is growing in unexpected ways,[9] it is necessary to rethink the fundamentals of investment in security and control. It is no longer control of access that makes the difference but rather control of use, meaning that people are all-important as the determining factor in improving the treatment of information via trustworthy and ethical criteria according to their context and the realities of the organization.

In this regard, the education required at present for individuals, rather than exercises or presentations on the procedures necessary for the protection of information (although necessary to learn about and understand the reason for their existence) or playful performances or award ceremonies for exemplary behavior, should teach employees to understand their environment and how their actions may affect both their personal reality and that of the organization. That is, individuals must personally assume responsibility for the risk to which the organization's digital assets are exposed and how their behavior makes a difference in the creation of the perception of reliability and trust, with the former based on the reality of vulnerability.

Data Security Education: A Challenge of the Appropriation of Difference

Research and practice in general insist that people are the most important element in data security, but this is paradoxically the area with the lowest amount of organizational investment in terms of security/cybersecurity. One possible explanation for this tendency lies in the technical and operational priorities of organizations with regard to maintaining current infrastructure, renewing licenses and updating technical tools; all of which occupy much of the attention of heads of security and engender the ideal of trustworthiness that executives have of security and control.

In this counterintuitive scenario, a series of everyday practices is implemented at organizations with the hope that individuals will acquire a set of behaviors that corresponds to the expectations the organization has around safeguarding its digital assets.

The first practice is trainings. Training is a meeting called to provide information on the organization's processes and practices concerning data protection. The guidance received should tell people how the relationship is, how to handle the information the organization possesses and what is expected of them in terms of the level of access they have, with the attendant consequences of any acts that go against specific instructions. These types of activities are generally offered to employees as part of the onboarding processes

© 2019 ISACA. All rights reserved. *www.isaca.org*

> IT IS NO LONGER CONTROL OF ACCESS THAT MAKES THE DIFFERENCE BUT RATHER CONTROL OF USE.

when they are hired by organizations and are followed up by periodic actions to remind them to bear this in mind in their day-to-day practice.[10]

The second practice is frequently referred to as raising awareness. This type of activity seeks to use concrete actions and experiences to train people in the procedures and access controls in such a way that they can develop practical skills and knowledge of how such controls make the idea of control a reality. These types of exercises are done directly in the work area to contextualize control actions in people's everyday tasks and to recognize how it is possible to ensure that the specific business processes around the handling of data are adhered to by everyone.[11]

The third practice is not often mentioned and deals with something more interior to people: appropriation.[12] This practice does not seek to inform or train the employee, but rather to construct a transcendent meaning and mission for the protection of information. The construction of a series of learnings and unlearnings makes it possible to act according to ethical, responsible principles that go beyond control of access (an exterior measure) to factor in control of use (an interior measure). This type of approach seeks to connect individuals with their responsibility for the results of their decisions and actions in relation to data security; that is, the recognition and acquisition of a personal differentiation of why and to what end employees should protect the organization's digital information.

Of the three practices mentioned, the first two have been used (and continue to be used in organizations) to try to change people's behavior and train them to conform to the expected treatment of information. In these endeavors, individuals experience security fatigue, a weariness of the insistence on the subject, generally embodied by a sense of resignation, loss of control, minimization of risk and evasion of decision-making.[13] These as manifested in the domain of material resistance[14] are demonstrated by:

- The presence of internal irregularities or discontinuities (i.e., regulatory changes, administrative changes, staff movement, bad business results)
- Irregularities originating in the practice of the business itself (i.e., updating of responsibilities, changes in the way tasks are done, adjustments due to the incorporation of information systems and technologies, cases of corruption)
- Changes in business geometry (in the model of value creation) and the operational environment or emerging threats

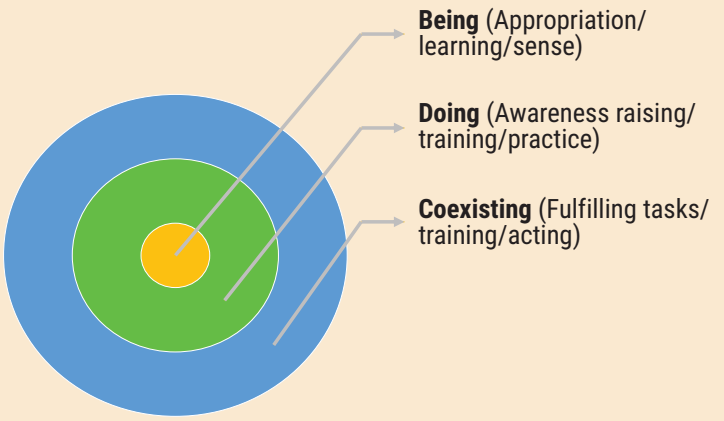
These can lead to individuals' rejection of security and control questions, which are generally based on specific terms of practice associated with international standards rather than the language of business, thus creating a greater distance between business areas and security professionals.

Figure 2 shows that despite an insistence on coexistence and practice as a basic exercise in security/cybersecurity education, a new distinction cannot be made that makes sense to people involved in data protection. People create distinctions that they adopt as their own and which go beyond their prior knowledge both when efforts are concentrated on the creation of meaning based on their learning or unlearning and when it is possible to surprise them and suspend the exercise of reality[15] in relation to security matters.

One book posits a process of investigation that aims at "action to improve" through social learning.[16] That is, understanding the problematic situation of security challenges, remembering actions previously carried out, designing new intentional activities based on a model of understanding current reality, using the proposed model to ask questions of and challenge the reality and, ultimately, obtaining different answers with two features:

© 2019 ISACA. All rights reserved. *www.isaca.org*

Figure 2—Security/Cybersecurity "Education" in Organizations



- Desirable, based on the model constructed
- Feasible, which is associated with the history, culture and personal dynamics of the persons taking part

In this way, when a space for learning and discovering data security is created—not to follow an established script, but rather to understand the "why" of things—a learning window is created where mistakes are not something to be punished.[17] Instead, they represent an opportunity to consolidate a lesson learned or, better yet, to express freely, openly and authentically those blind spots that the organization is unaware of due to the very nature of its dynamics.

Molding Human Behavior in Security/Cybersecurity

Strengthening people's education in security/cybersecurity inside organizations represents an important step in consolidating a concrete distinction in the protection of data assets. It also creates a scenario for the emergence of that which the organization requires and desires in order to tackle the challenges of reliability and trust that customers demand in an ever more hyper-connected environment.

Recent research has established that at least five elements (**figure 3**) are required to mold people's behavior in relation to security and control:[18]

- Preparation
- Responsibility
- Management
- Social elements
- Regulation (this last element is not included in the original model)

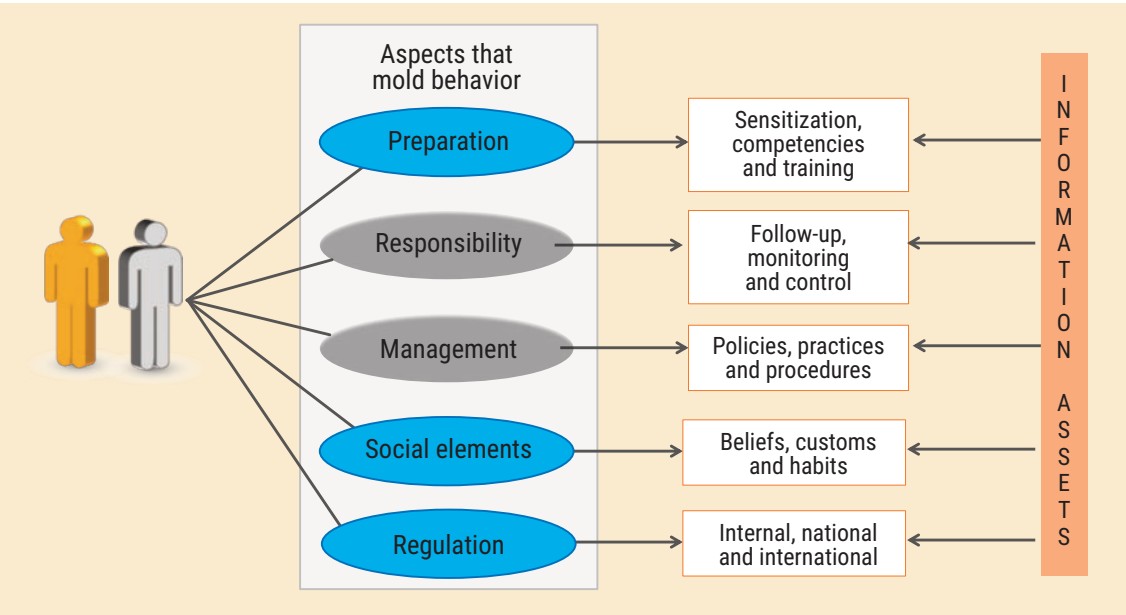
> "MANAGEMENT IS THE PRACTICE OF SEEKING TO INCREASE THE CERTAINTY AND REPEATABILITY OF THE ORGANIZATION'S SECURITY AND CONTROL ACTIVITIES."

In this context, the term "mold" should be understood as configuring a personal vision of the assets in a systematic way so that the elements of coexisting, doing and being are composed around an overarching mission that the organization has managed to connect to each of the participants in a transparent, authentic way.

Preparation implies developing competency in the secure management of information,[19] which makes it possible to establish levels of perfection and mastery in the protection of data. It also guides people toward an understanding of practices and how to implement them consistently in the real world of business and to recognize their autonomous, concrete responsibilities, knowing that both the organization and they themselves can have a psychologically safe environment in which to act when things do not work out as planned.

© 2019 ISACA. All rights reserved. *www.isaca.org*

Figure 3—Aspects That Shape Information Security Behavior



Individual responsibility based on the personal distinctions constructed by each participant must be assisted by the recommended practice of the standards for follow-up, monitoring and alerting in such a way that both the execution of the activities in the processes and the decisions that people make occur within a framework of verification. This framework is designed not to assign blame, but rather to limit the effects on customers, which can then be translated into lessons learned and potential new scenarios of possible fatigue of the current security distinction.

Management is the practice of seeking to increase the certainty and repeatability of the organization's security and control activities. It is the traditional exercise relating to the quality cycle—planning, doing, verifying and acting—that seeks to homogenize the organization's intended effects in order to avoid surprises. Although these are activities that constitute the minimum requirement for greater trust, they do not solve the equation of the inevitability of failure. In short, it is the least that can be done.

Social elements have to do with each individual's reality. Recognizing people's beliefs, customs, rituals and habits with regard to the treatment of data represents a valuable resource for fine-tuning and strengthening the competencies required for data protection. To understand the social fabric in which people's behaviors manifest themselves is to discover the fine lines of the imaginaries that individuals create and end up acting on in diverse situations.

Regulation is the normative element; the demand of third parties to ensure the function of compliance. People in charge of compliance at organizations are responsible for, among other things, developing the culture, anticipating risk, ensuring operation and consultation, and implementing best practices. These activities are designed to observe the guidelines laid down by supervisors in different sectors to enable the organization to project an image of imperfect trustworthiness[20] that tells its different interest groups it is capable of taking on the responsibility of protecting its information assets and the interest groups themselves.

These five components act in harmony and are based on three evolutionary cycles:

- **Regulation**—Which safeguards today
- **Adaptation**—Which focuses on tomorrow and renews the present[21]
- **Memory and learning**—Which challenges previous knowledge, compares present results and establishes the basis for the formulation of a change in people's behavior

© 2019 ISACA. All rights reserved. *www.isaca.org*

> FINDING NEW ANSWERS TO THE CHALLENGE OF DATA SECURITY BEHAVIORS DEMANDS MOVING BEYOND WHAT IS CURRENTLY KNOWN ABOUT RAISING AWARENESS AND COMPLIANCE.

This means overcoming an individual vision of a person's actions to establish a system of relationships constructed according to an individual's view of a community, where one's responsibilities are governed according to an understanding and recognition of others' vulnerabilities.[22]

Conclusion

Analyzing the human factor in data security is not a task that involves the disciplined viewpoint of a profession or a particular reading of a presently available standard. It is instead an exercise that demands moving beyond a mechanistic, limited vision and attempting to configure a homogeneous understanding of people organized around basic norms who say and know how security and control are done.

Finding new answers to the challenge of data security behaviors demands moving beyond what is currently known about raising awareness and compliance, two distinctions that have imposed themselves on security discourse, which frequently ends up exhausting people's practices and causing discomfort to collaborators across areas with its talk of risk and the threat of undesired events.

Strengthening people's practices and behaviors means recognizing where vulnerabilities occur, what are the most critical attack vectors, and developing safe data management practices that connect with people's realities and with the essence and sense of protection of an organization's information assets. It is an effort that seeks to understand the inevitability of failure as a reality and to take advantage of each of the lessons learned in order to reinvent the distinctions of information security that people make and motivate them to look beyond current procedures and standards.

Transforming people's behavior toward data security depends on connecting three evolutionary cycles that make the present function in accordance with established practice; make the future an exercise in construction and collective practice that visualizes challenging, potential and plausible scenarios that prepare the organization for emerging threats and risk; and make learning (or unlearning) the very essence of the way in which reality is dismantled to disconnect what now exists to incorporate the novelty of what is coming and to reconnect the dots in ways that are completely diverse and novel.

Consequently, the human factor in security/cybersecurity must cease to be dead emotional weight that security and control executives carry but do not know what to do with, instead becoming strategic leverage in their programs for the protection of digital and informational assets that are in a constant process of development. Thus, the human factor becomes a "reliable and resistant factor" in the organization's security/cybersecurity system, something that demands an emerging vision by security/cybersecurity professionals of themselves as new educators who, paraphrasing John Ruskin, say, "Do not teach something to someone who doesn't know, but rather transform them into something that didn't exist."[23]

Endnotes

1. "Chain" is defined here as the sequence of connected links that enables a system to function. Its strength is defined in terms of the connection that is least strong.
2. Dreyer, P.; T. Jones; K. Klima; J. Oberholtzer; A. Strong; J. Welburn; Z. Winkelman; "Estimating the Global Cost of Cyber Risk: Methodology and Examples," Rand Corporation, 2018, *https://www.rand.org/pubs/research_reports/RR2299.html*
3. Alhogail, A.; A. Mirza; "Information Security Culture: A Definition and a Literature Review," World Congress on Computer Applications and Information Systems, Hammamet, Tunisia, 17–19 January 2014

© 2019 ISACA. All rights reserved. *www.isaca.org*

4 Bada, M.; M. A. Sasse; J. R. C. Nurse; "Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour?" *International Conference on Cyber Security for Sustainable Society*, 2015, *https://arxiv.org/abs/1901.02672*

5 Fuenmayor, R.; H. López-Garay; "The Scene for Interpretive Systemology," *Systems Practice,* vol. 4, iss. 5, 1991, *https://doi.org/10.1007/BF01104459*

6 Kuper, P.; "The State of Security," *IEEE Security & Privacy*, September/October 2015, *https://doi.org/10.1109/MSP.2005.134*

7 Cano, J.; "Administrando la Inseguridad Informática," *Revista Hakin 9*, vol. 23, iss. 4, 2007, *https://es.slideshare.net/heynan/hakin9-inseguridad*

8 Kuper, P.; "The State of Security," *IEEE Security & Privacy*, vol. 3, iss. 5, September-October 2005, p. 51-53

9 Sieber, S.; J. Zamora; "The Cybersecurity Challenge in a High Digital Density World," *European Business Review*, 18 November 2018, *https://www.europeanbusinessreview.com/the-cybersecurity-challenge-in-a-high-digital-density-world/*

10 Wilson, M.; J. Hash; *Building an Information Technology Security Awareness and Training Program*, National Institute of Standards and Technology Special Publication (SP) 800-50, USA, 2003, *https://csrc.nist.gov/publications/detail/sp/800-50/final*

11 *Ibid.*

12 Alnatheer, M.; *Understanding and Measuring Information Security Culture in Developing Countries: Case of Saudi Arabia*, Queensland University of Technology, Australia, 2012, *https://eprints.qut.edu.au/64070/*

13 Stanton, B.; M. F. Theofanos; S. S. Prettyman; S. Furman; "Security Fatigue," *IT Professional*, vol. 18, iss. 5, 2016, *http://doi.org/10.1109/mitp.2016.84*

14 Ingemecanica, "Mechanical Resistance to Fatigue: Tutorial No. 217," *https://ingemecanica.com/tutorialsemanal/tutorialn217.html*

15 Reyes, A.; R. Zarama; "The Process of Embodying: A Re-Construction of the Process of Learning," *Cybernetics & Human Knowing*, vol. 5, iss. 3, 1998, *https://www.researchgate.net/publication/233613109_The_process_of_embodying_distinctions_a_re-construction_of_the_process_of_learning*

16 Checkland, P.; J. Poulter; *Learning for Action: A Short Definitive Account of Soft Systems Methodology and Its Use for Practitioners, Teachers, and Students*, John Wiley & Sons, England, 2006

17 Schoemaker, P.; *Brilliant Mistakes: Finding Success on the Far Side of Failure*, Wharton Digital Press, USA, 2011

18 Ahmad, Z.; T. Ong; T. Liew; M. Norhashim; "Security Monitoring and Information Security Assurance Behaviour Among Employees: An Empirical Analysis," *Information & Computer Security*, 12 June 2019, *https://doi.org/10.1108/ICS-10-2017-0073*

19 Cano, J.; "Gestión Segura de la Información: Competencia Genérica Clave en una Sociedad de la Información y el Conocimiento," *Memorias Congreso Internacional de Educación, Tecnología y Ciencia, CIETyC*, vol.3, iss. 1, 2015, *https://www.researchgate.net/publication/334602391_Gestion_segura_de_la_informacion_Competencia_generica_clave_en_una_sociedad_de_la_informacion_y_el_conocimiento*

20 Cano, J.; "Riesgo y Seguridad: Un Continuo de Confianza Imperfecta," *Actas IX Congreso Iberoamericano de Seguridad de la Información*, Universidad de Buenos Aires, Spain, 2017, *https://www.researchgate.net/publication/321197873_Riesgo_y_seguridad_Un_continuo_de_confianza_imperfecta*

21 Espejo, R.; A. Reyes; *Sistemas Organizacionales: El Manejo de la Complejidad con Modelo del Sistema Viable*, Ediciones Uniandes—Universidad de Ibagué, Colombia, 2016

22 Brown, B.; *El Poder de Ser Vulnerable: ¿Qué Te Atreverías a Hacer Si el Miedo No Te Paralizara?* Ediciones Urano, Spain, 2016

23 Ruskin, J.; "Quotable Quote," Goodreads, *https://www.goodreads.com/quotes/287586-education-does-not-mean-teaching-people-what-they-do-not*

© 2019 ISACA. All rights reserved. *www.isaca.org*