ISSN: 2687-8402

DOI: 10.33552/OAJAA.2020.02.000535

Open Access Journal of Archaeology and Anthropology

Iris Publishers

Opinion

Anthropological Take on Cyber-security: How a Legacy Security Belief System is Impacting Us Today

Susan Squires* and Jamie Johnson

Department of Anthropology, University of North Texas, USA

***Corresponding author:** Susan Squires, Department of Anthropology, University of North Texas, USA

Received Date: April 29, 2020

Published Date: May 12, 2020

Opinion

Between 70% and 97% of all cyber breaches can be attributed directly or indirectly to human errors (Ponemon Institute 2018) [1]. In this opinion piece, we explore the archeology of cyber-security embedded in 20th century legacy belief and its artifacts.

During the "formative period" of the computer in the last quarter of the 20th century, computers became generally available to a few societies that existed at the time. Archaic documents, such as early advertisements and bills of sale, confirm the spread of these early tools from places of work to domestic spaces. From histories we know that such computers were primarily stand-alone devices. If connected, modem-mediated access to the early Internet was conducted through telephone lines, which provided a mechanism for sending emails to immediate kin, friends or workgroup members.

Individuals who operated computers were called users. Many of our present ideas about the relationship between people and computing technology were formulated by users during this proto-Internet era. There arose a class of indigenous experts with specialized knowledge dubbed Human-Computer Interactions (HCI). These specialists canonized the foundational beliefs for ensuring usability of computing technology by codifying HCI rules Laurel [2] and design principles Norman [3]. While formulaic at the time, dogmatic beliefs about security centered on the stand-alone device and its user. To safeguard personal computers, the password was created to ensure other users could not access personal or work-related data saved on the hard-drive. Rogue programs, like The Real-time Operating system Nucleus (TRON), targeted individual users' programs on their machines.

We now live in an 'always on' interconnected world. Since that formative time, society has experienced a massive shift from traditional small-scale communication with kin and close workgroup members to a world-wide human communication system that has extended kinship networks, created legions of fictive kin, replaced friends with contacts and followers, and workgroups with virtual teams located around the world. Communication media and the Internet now serve as the backbone for virtually all facets of modern life, from personal communications and finance to the processing and management of electrical grids and power plants Brodsky and Radvanovsky [4], Rege-Patwardham [5]. As Tom Holt and Adam Bossler recognized in their article, An Assessment of Current State of Cybercrime Scholarship (2014), these innovations spurred massive changes in our perceptions of personal expression and social interaction (Figure 1).

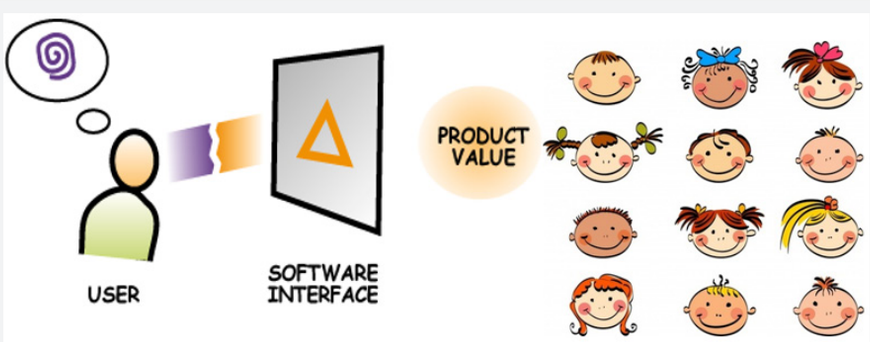

Figure 1

With growing "connectivity", the relationship people have with technology has evolved from a human – computer interaction (HCI) to a human-machine-human (HMH) entanglement Hodder [6], Bryant [7]. While our communication system evolved, the legacy of the beliefs and patterns of use remain buried, obscured by decades of computer artifacts.

The Human Computer Interaction paradigm is a legacy belief system that no longer best describes the multimodal digital interfacing or multi-local human relationships, which previously informed cyber-security risk prevention. Despite our awareness of this new group dynamic, it appears as though the dogma endures. As anthropologists are aware, beliefs systems are conservative and change at a much slower rate than technology. If we are to see a shift in culture, it must begin by creating new paradigms, which fundamentally change how we think, talk, and act toward cyber security [8-10].

It is paramount that this paradigm shift recognizes HCI obsolescence: an artifact of the past. Interactions are now with other humans, their machines, their systems, and their organizations. Embracing security concerns means thinking about cyber-security as a non-linear, interconnected, large-scale and complex context that now spans groups, organizations, and society as well as individuals. If we are to truly re-design cyber-security, we will even need to abandon words such as user, which suggests individual responsibility, and move to concepts such as member and collective, which more accurately reflects the interconnected social networks of people. For always-connected communities, transactional cyber-security precautions, such as passwords or firewalls, constitute not merely a nuisance, but a legacy barrier to interactions: barriers to culture change to be overcome.

This more holistic anthropological approach to interactive types of cyber-security must take into account

i. Collective level beliefs and values that shape decisions and subsequent behaviors,

ii. The social information systems that transmit and reinforce knowledge,

iii. Organizational level structures including but not limited to cost-benefit incentives and policy interventions, and

iv. Integrated technical systems that can provision appropriate human solutions.

Acknowledging the interactional component with a collective character will open new avenues of research that warrants further exploration including new conceptual frameworks, that situated individuals within the context of community rather than using context as the stage for individual decisions. This is a complex research problem if we are to re-design cyber-security on the collective level - organization and society. An anthropological position situates the problem precisely to understand and support the goals of the collective, not just the individual. The challenge will be to canonize new dogma, which is based on our understandings of culture, for this emerging socio-technical system where there is a recognized "reciprocal relationship between technology and people" (STAST).

References

1. (2018) Ponoman Institute, USA.
2. Laurel Brenda (1990) The Art of Human-Computer Interface Design. Addison-Wesley, USA.
3. Norman Donald (1988) The Design of Everyday Things. Basic Books, New York, USA.
4. Brodsky J, R. Radvanovsky (2011) Control Systems Security. In T. J. Holt and B. Schell (Eds.), Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications, IGI Global, PA, USA, pp. 187-204.
5. Rege-Patwardham, A (2009) Cybercrimes against Critical Infrastructures: A Study of Online Criminal Organization and Techniques. Criminal Justice Studies 22: 261-271.
6. Hodder Ian (2011) Wheels of Time: Some Aspects of Entanglement Theory and the Secondary Products Revolution. Journal of World Prehistory 24(2/3):175-187.
7. Bryant, Levi R (2014) Onto-Cartography: Ontology of Machines and Media. Edinburgh: Edinburgh University Press, UK.
8. Holt, Thomas, Adam Bossler (2014) Cybercrime. Oxford Handbooks Online, South America.
9. Jessop Bob, Neil Brenner, Martin Jones (2008) Theorizing Sociospatial Relations. Society and Space 26(3): 389-401.
10. (2020) Socio-Technical Aspects in Security, UK.