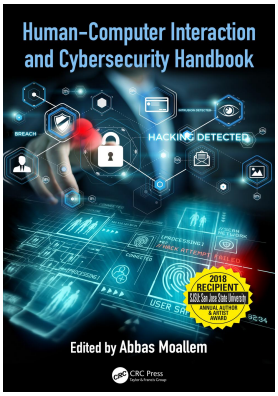

Human-Computer Interaction and Cybersecurity Handbook

Abbas Moallem

Perspectives on the future of human factors in cybersecurity

Publication details
https://test.routledgehandbooks.com/doi/10.1201/b22142-19
Abbas Moallem
Published online on: 24 Oct 2018

chapter nineteen

Perspectives on the future of human factors in cybersecurity

Abbas Moallem

Contents

19.1 Introduction

Computer technology is rapidly changing, and the world will soon be connected in one way or another to the Internet. Personal, enterprise, and government information will be digitalized from its physical (paper documents and printed image) form. As this is already happening in the more industrialized countries, we can now predict that sooner or later, all countries, poor or rich, will be joined to this network.

We also can predict that many technological solutions will be found to increase the protection of the digital assets of individuals, groups, and organizations. However, with more people connecting to this huge network, more individual vulnerability will also result. In the field of cybersecurity, the prediction is that this is to be a growing field, and one might assign the same likelihood to the importance of human factors in cybersecurity.

In this chapter, after providing a summary of future perspectives on the future of human factors in cybersecurity, the perspective of each contributor is extracted from their chapter and presented as a separate subsection.

19.2 Summary

19.2.1 Authentication

- Authentication in the future: Authentication will no longer be dominated by passwords. Consequently, users should expect authentication with less pain and more ease in the future.
- Authentication will still use "something you have, something you know, and something you are."
- Biometric usage has the potential of greatly improving cybersecurity, because it relies on inherent biological traits rather than knowledge factors for authenticating or identifying users.
- Biometric verification will increase in use in combination with other methods of identity proofing and authentication.
- With the accumulation of different biometrics information, privacy will be the main future challenge.
- Biometric characteristics will likely become extensively used for biometric verification, but if the site implements effective attacks detection, then using stolen biometric data to authenticate might not work. However, the main privacy challenge arises from other usage. For example, facial images might be used to link a user's account to the user's activity on social networks or the user's visit to a physical store equipped with customer identification cameras.
- The keys and digital certificates are going to get more mature and be used to secure sensitive data, protect its integrity, and authenticate the participants in any digital interaction.

19.2.2 Trust and privacy

The need to elaborate new theories, methods, and research to understand how human and nonhuman team members work most effectively in cybersecurity context will grow.

- Disruptive innovations will have more impact on society with mass deployment.
- Worries will grow regarding privacy and exponential increases of mass data collection from all aspects of the human's life.
- Storage of data in the cloud, i.e., centralized repositories, and predictive analysis of collected data will be a big area of concern.
- Big data will be analyzed by machine learning techniques to provide detailed, personalized characteristics of an individual and prediction of individual future behavior.
- The control on data stored will be the main concern of all human societies, countries, organizations, and human communities.
- Predictions with 99% accuracy based on big data analysis will result in concerns for the 1% of predictions that are inaccurate and wrong. One percent of a population of 50 million is still 500,000; that is not a negligible number, and such error rates associated with big data analysis may be intolerable.
- People whose privacy is violated are vulnerable to manipulation. In dictatorships, people behave according to the dictator's wishes because of fear preventing them from doing something else. In western democracies, this issue will not be less dangerous.

- The needs for tools that facilitate human decisions and responses based on data will grow. Consequently, such tools will provide tremendous power for the cybersecurity professional.

19.2.3 Threats

- The insider threat might not be as frequent as malicious software, but its impact can be costly.
- Big data analytics and the incorporation of personality traits, psychological factors, psychosocial data, and motivations in profiling might be used to prevent insider events.
- Social engineering is going to be an evolving practice with many new perpetrators.
- Social engineers use well-known techniques and continually explore to find new ways to use human behavior to exploit the weakness in people unable to distinguish lies from truth to acquire information.
- As more consumers shop and pay with connected devices, and commerce increasingly migrates to digital channels, industries need to invest and invent new standards, technologies, and products to remove sensitive account data from the payment environment, putting it into a form that cannot be used by criminals for fraud. Products, services, and online platforms should develop built-in security and privacy features, thereby protecting both the product and the customer information from being hacked.

19.2.4 Smart networks and devices

- Security in home networking devices will improve first by making the settings and configurations of the home networking device more user-friendly and increasing user awareness on security.
- Ambient assisted living (AAL) applications for supporting the aging will still expand, particularly the usage of Internet of things (IoT) technologies.
- The needs for regulations on IoT are going to be growing.

19.2.5 Governance

- The need for more laws and regulations with regard to technology, cybercriminality, privacy, and particularly IoT will increase in all modern societies. The regulations will have a huge impact on our daily lives, affecting how we work and protect our children.
- The need to address cybersecurity in our daily lives, for our work, and to protect our children will grow.
- Everyone will need to have the basic understanding of how security and privacy are handled in the law, in technology, and in government.
- Legislative efforts on cybersecurity and privacy will continuously grow.

In the following section, the perspectives of the authors and experts in each area are provided.

19.3 Authentication and access management

In terms of authentication, according to Furnell (Chapter 1),

> one thing we can be sure about moving forward is that the authentication landscape will no longer be as dominated by passwords as it has been in the past. The use of alternative approaches (particularly biometrics) has already become commonplace, so users can expect a far more varied experience than they have previously been offered. Moreover, if the technology choices are appropriately judged and correctly matched to their needs, then users should be able to expect authentication to feel less of a barrier to legitimate use. The options and opportunities are there—but they still require manufacturers and service providers to take them.

Corella (Chapter 2) believes that

> cybersecurity depends on the integrity of computer systems and their operation by human users and administrators. The most dangerous cyber attacks are those that target both system and operational vulnerabilities, leveraging system exploits to compromise user accounts, or compromising systems by impersonating users or modifying their behavior using social engineering techniques. The science of human factors is concerned with the interaction between humans and computer systems, and therefore has key contributions to make towards strengthening cybersecurity. One of those contributions will no doubt be an acceleration of the ongoing research on biometrics.
>
> Operational vulnerabilities derive primarily today from the reliance on knowledge factors to identify and authenticate users, either knowledge of secret passwords or knowledge of private information used in automated knowledge-based verification or human-to-human interaction. Passwords are still the most common means of authenticating users on the Internet, despite many efforts to replace them, and knowledge-based verification is still the primary means of remote identity proofing.
>
> Biometrics is a disruptive technology that has the potential of greatly improving cybersecurity, because it relies on inherent biological traits rather than knowledge factors for authenticating or identifying users. Biometric authentication is not vulnerable to phishing attacks or breaches of backend databases. Even if an adversary breaches a database of user accounts containing facial images, the adversary will not be able to use one of those facial images to impersonate a user unless he or she is able to prove to a verifier that the image is that of his or her face.
>
> But the security gains promised by biometrics depend on the ability to thwart spoofing with effective presentation attack detection, which is difficult. Recent advances in deep neural network technology have yielded remarkable improvements in the accuracy of

facial image verification, and similar improvements may be achievable in other biometric modalities. But such accuracy improvements are consistently reproducible only in non-adversarial settings and have been shown to be vulnerable to adversarially crafted images in spoofing attacks. Both neural networks and classical biometric technologies have to contend with powerful digital attacks such as voice morphing that construct virtual realities in real time and may thereby be able to respond to anti-replay challenges.

In biometric verification there will always be an arms race between verifiers and impersonators. Therefore, biometric verification should be used in combination with other methods of identity proofing and authentication, so that the emergence of an unforeseen method of attack is not catastrophic for the verifiers. The old mantra of proving your identity with "something you have, something you know, and something you are" remains valid.

While spoofing attacks pose a security challenge to biometric verification, a severe privacy challenge arises from the fact that the biometric characteristics used for biometric verification may be used to link the user activities across both cyberspace and the physical world. An adversary who breaches a web site's user database containing facial images may not be able to impersonate users if the site implements effective presentation attack detection but may be able to use the facial images to link each user's account to the user's activities on social networks or the user's visits to physical stores equipped with customer identification cameras.

The privacy challenge may be addressed by two distinct avenues of research. One of them is continued research on revocable biometrics, also known as biometric cryptosystems, which rely on randomized and revocable helper data that is deemed to reveal no useful biometric information, in lieu of traditional biometric templates. The other is research on biometric architectures that do not make use of databases of biometric information. In one such architecture, commonly used today in mobile devices, biometric verification data is kept within the user's device, in local storage that provides some resistance to physical tampering and/or malware. In another architecture that dispenses with biometric databases, biometric verification data is included in a hybrid crypto-biometric credential issued by a certification authority.

All this means that biometrics will be a most active area of research for the foreseeable future, concerned with presentation attacks and their detection, revocable biometrics, biometric verification architectures, new biometric modalities, and improvements of neural network robustness in adversarial settings.

Nair (Chapter 3) believes that

> keys and certificates are poised for explosive growth fueled in part by trends in virtualization, cloud, DevOps, and IoT. Yet they are also among the least understood concepts of cybersecurity, as evidenced

> by the low investment in good cryptography management practices. This is especially stark when compared to the billions of dollars we spend as an industry to protect older, less secure technology such as usernames and passwords.
>
> It is because of this lack of awareness that malicious actors, whether it be private groups of individuals or nation states, target vulnerabilities in the implementation of cryptographic security—SSL/TLS attacks dwarf all other forms of network attacks today, and this difference will only continue to grow. The technology itself is mature and, when implemented correctly does what it is supposed to do, it secures sensitive data, protects its integrity, and authenticates the participants in any digital interaction. This robustness of the technology is now being utilized for malicious purposes, leading to an ongoing debate between the benefits afforded by security/confidentiality on one hand and the threats they pose to citizens from all walks of life on the other.

19.4 Trust and privacy

Cellary (Chapter 4) states that without the science and methods of human–computer interaction (HCI), new tools are not likely to support effective decisions. Consequently, HCI will also need to elaborate new theories, methods, and research to understand how human and nonhuman team members work most effectively in cybersecurity contexts.

> Thoughts regarding future perspectives of e-privacy: Disruptive innovations start to have impact on society only when they are deployed on a mass scale. Currently we are witnessing the mass collection of digital data in the clouds, i.e., centralized repositories, and predictive analysis of collected data. An individual is likely to be conscious of the collection of some data concerning him or her, but not all. He or she is conscious of data entered by him or her into computers to receive a required digital service. However, he or she is not conscious of data collected automatically by devices like cameras or sensors deployed in smart environments. Collected data, even if originally anonymous, may be quite easily attributed to identified individuals. Those data are then combined with data concerning millions of other individuals, products, services, situations, behaviors, reactions, etc., comprising big data. Big data may be analyzed by machine learning techniques to provide detailed, personalized characteristics of an individual and prediction of his or her future behavior. Given the state of the art of information technology briefly depicted above, we may now ask questions about the human and social consequences. It is clear that any institution (and its leaders), which has the possibility to use the above technology, can gain extreme power over individuals and societies. A question arises, who will these people and institutions be? Will society have control of such an institution? The question of control is very pertinent, as machine learning is not based on a cause-and-effect relationship, but on correlations among different datasets and analysis of a big number of training examples.

> If one mathematician proves a theorem, another mathematician may check the proof and find errors, if any. If a human programmer writes a program, another human programmer may inspect program code and find errors, if any. However, if a neural network is trained by peta-bytes of data, nobody is able to check whether a particular prediction is correct or not. If big data analysis provides predictions with 99% accuracy, which is great, there are still 1% of the predictions that are wrong. Taking the United States, whose population is 320 million, as a case, wrong predictions would concern 3.2 million people; that is huge. If a wrong prediction concerns advertisement of a product being uninteresting for an individual, the consequences are probably negligible. However, if a wrong prediction concerns a medicine or a medical procedure, the consequences for a patient may be very severe. Wrongly applied predictions may undermine principles of the judicial system. Currently, an individual is guilty if he or she committed a crime in the past and that fact was proved in the court. Prediction based on big data analysis with 99% or even higher accuracy that an individual will commit a crime in the future is not sufficient to pronounce him or her guilty, because the crime must really happen first. An approach based on predictions is motivated by a will to protect the possible victims of prospective crime, but neglects the free will of an individual who finally decides to commit a crime or not. Predictive big data analysis may also corrupt democratic political systems. People whose privacy is violated are vulnerable to manipulation. In dictatorships, people behave according to the dictator's wishes because of the fear that prevents them from doing something else. In the case of the mass deployment of big data analysis, people will behave according to self-fulfilling predictions because they will not be able to imagine anything else.
>
> The problem of e-privacy is so difficult to solve, and so important to study because there are no effective technical means at this time to protect e-privacy. In the past, similar problems have been solved by establishing proper laws forbidding actions that were inacceptable by a society concerned. However, the digital world is global, so a law established in one country is ineffective in other countries. Therefore, representatives of one country may violate e-privacy of citizens of other countries and manipulate them. To protect the privacy of people in a global digital world, a global law should be established and respected. This is unfortunately rather utopic.

Schuster and Alexander (Chapter 5) believe that the future of

> cybersecurity is a challenging problem because of its massive scale and rapid rate of change. The pace of technology makes it hard to predict what cybersecurity will look like in even the near future. We think it is a bit easier to envision how innovation in HCI will play a role in cybersecurity solutions. In the future, HCI will include greater use of naturalistic interfaces and the use of big data. These interfaces will become disruptive when they become highly accurate

> and robust. Our tools will feel as though they behave intelligently; they will anticipate our needs and adapt to us and our situations. This vision of naturalistic communication and higher-level tasks performed by automation is called human-automation teaming. Future automation for cybersecurity will talk to us and listen to us. It will understand higher-level tasks and appreciate the context of problems. Cybersecurity work will continue to require automated tools, but we will interact with them almost as though they are human team members. The ability to adapt responses to context and collaborate on human terms will facilitate human decisions and responses based on data. We imagine such a tool will provide tremendous power for the cybersecurity professional. In our vision, there will continue to be a need for effective human decision-making, but the nature of this work will be dramatically different than seen today. This power would also be available to the attacker. Thus, we do not suggest that human-automation teaming alone would change the cat and mouse game between attackers and defenders.
>
> However, the game might be disrupted if HCI innovation is combined with technological approaches to the problem. For example, an automated cyber defender teammate might allow analysts to rapidly identify novel attacks. Therefore, the future of cybersecurity depends on continued interdisciplinary science and practice, with HCI playing an important role. Without the science and methods of HCI, new tools are not likely to support effective decisions. HCI will also need new theories, methods, and research to understand how human and non-human team members work most effectively in cybersecurity contexts.

19.5 Threats

Papadaki and Shiaeles (Chapter 6) think that

> the insider threat might not be as frequent as malicious software, but its impact can be costly. Detecting insider threats is not a purely technical solution, and the human factor can play an important role. Recent research has recognized its importance and has incorporated personality traits, psychological and psychosocial data, as well as motivations and possible catalysts of insider events. Beyond prevention and detection, though, best practices and guidelines recognize that insider threat is a multifaceted problem, and the success of insider threat mitigation strategies depends on the cooperation of various groups within an organization. Specifically, specific emphasis is given on management, human resources, legal, physical security, data owners, IT, and software engineering.

On social engineering, Moallem (Chapter 7) believed that

> it is an evolving practice with many sources of new perpetrators. Social engineers use well-known techniques and continually explore

> to find new ways to use human behavior to exploit the weakness in people unable to distinguish lies from truth to acquire information. Until technology offers automatic solutions to help users in detecting the lies and protecting people from being victims of social engineers, users will be required to gain awareness and knowledge to protect themselves from deception techniques. Cybersecurity experts should be constantly evaluating and detecting tactics of social engineering and providing efficient warning and training to protect personal and organizational assets.

With regard to money laundering and black markets, Bayatmakou (Chapter 8) believes that

> as more consumers shop and pay with connected devices, and commerce increasingly migrates to digital channels, industries must invest in new standards, technologies, and products. One of the best defenses is removing sensitive account data from the payment environment, putting it into a form that cannot be used by criminals for fraud. Products, services, and online platforms should develop built-in security and privacy features, thereby protecting both the product and the customer information from being hacked.

19.6 Smart networks and devices

The home network will have a huge impact on the life of each individual in the future. The (Moallem, Chapter 9)

> …router works as the front door to your digital data and due to the complexity of protecting systems, most home networks are very vulnerable. Security can be achieved first by making the settings and configurations of the home networking device more user friendly and intuitive to user needs. Secondly, there needs to be an increase in user awareness on security, along with basic trainings to how to properly manage a home network, at the very least to help users protect their system by enabling basic security settings.

Tragos (Chapter 10) thinks AAL applications for supporting the ageing will still expand particularly usage of IoT technologies. He believes that

> Human Computer Interaction and cybersecurity have a bidirectional relationship, which is very critical for future applications, especially in scenarios with people in the need. On the one hand, HCI needs cybersecurity mechanisms in order to ensure that the systems are secured and no unauthorized third parties can intervene and interact with computers in a malicious way. However, past research has worked a lot on identifying solutions to cybersecurity issues in HCI. Lately, the focus in the IoT world has shifted towards designing and developing trusted IoT systems. HCI can help on this by bringing the human factor closer to the IoT devices and assisting

> towards increasing the users' perception of trust in an IoT system. Most interfaces for management of IoT applications and systems are not user friendly and do not provide enough information about the status, any issues, emergencies or attacks. For an average home user, more user-friendly and simple interfaces should be developed, so that the user is able to easily understand if something is wrong in his environment and try to resolve the issue. Thus, HCI should also focus on improving the situational awareness of users with respect to cybersecurity issues in their environment.
>
> Another important thing for future research is how HCI can help improve cybersecurity. This becomes more important with respect to the privacy regulation of the European Commission that will take effect in May 2018 (GDPR).* According to this regulation that will become law in all EU countries, users should have full control over their data. HCI applications can provide significant assistance for the realization of interfaces so that technology-illiterate users will be able to understand in a simple, yet effective and interactive way the data they are sharing through all their devices and applications. Additionally, using simple interaction the users should be able to control their data, getting alarms for new requests to share data and managing the response to these requests. This is of utmost importance to ensure the requirements for privacy by design and privacy by default as described in the GDPR. Thus, HCI researchers should also work on this area of research, trying to work together with end-users to understand their requirements for designing user-friendly interfaces to improve the privacy of user sensitive information.

On attacks on smart cities, Staudemeyer (Chapter 11) believes that

> legal support should be expected to be needed to handle consequences and to initiate legal actions against the attackers. A root cause mitigation team could be engaged to investigate why a breach was possible and develop a mitigation plan that can be realized rapidly. This is an especially crucial step in battling cybercrime.
>
> *The life cycle, once implemented, will change with every iteration according to the needs of organization. With a proper privacy engineering organization in place, a solid privacy-by-design approach can be reached in system design as well as the operation of the IoT system. For smart cities, a proper privacy life cycle is a quality differentiator.*

Lau et al. (Chapter 12) believe that supervisory control and data acquisition (SCADA) will be still be a widely used control architecture for many industrial systems in the critical infrastructures. Thus, HCI research should try to enhance SCADA security

> through user interface design that supports workers in the effective configuration of security tools and acquisition of cyber SA. Further,

* GDPR: EU General Data Protection Regulation, http://ec.europa.eu/justice/data-protection/reform/index_en.htm.

> research must begin to focus on teamwork starting with staff in security and operations for coordinating response to cyberattacks. Finally, HCI could examine how the attribution and retribution of attackers may shift the asymmetry of cybersecurity in favor of the defenders.

19.7 Governance

Laws and regulations need to evolve to regulate technologies and issues that will include everything from criminality to data protection to protection of citizens' privacy.

Schertler (Chapter 14) thinks that

> in the coming years, we will all become Carrie from Homeland. We will need to address cybersecurity in our daily lives, for our work and to protect our children. A basic understanding of how security and privacy are handled in the law, in technology, and in government policy will be useful for thriving in the coming cybercentury.

And Jill Bronfman (Chapter 14) put it in more poetic terms:

> What of ourselves are we willing to sacrifice for comfort?
> For safety?
> For security?
> To see the future, we look past the past
> I'll miss you: hand-held remote control, power cord, steering wheel,
> Or not.
> The past is perhaps not only prologue
> But epilogue
> Surprise me

In terms of regulation, Quirchmayr (Chapter 15) emphasizes that

> recent and ongoing legislative efforts around the globe stress the continuously growing importance of cybersecurity and privacy. Security by design and security by default will be mandated by EU legislation from May 2018 with respect to the protection of personal data. The importance of HCI in cybersecurity will, therefore, increase significantly, among other reasons, because it will be a core factor in achieving legal compliance.

With the expansion of Internet of things Weber (Chapter 16) believes that

> cybersecurity plays an important role in the data processing/collecting context of the Internet of Things (IoT). Governmental regulations can build a certain normative framework, but human factors must also be aligned to the cybersecurity challenges. In the European Union (EU), the Network and Information Security (NIS) Directive of 2016 has the objective of implementing a "culture" of security elements for the benefits of citizens, consumers, businesses

> and public sector organizations. The NIS concept encompasses the ability of networks and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of processed, stored or transmitted data or related services.
>
> The term *culture* highlights that human factors must be taken into account in connection with the main topics and measures that can realize the desired level of information security, namely the improved national cybersecurity capabilities, the improved cooperation between governmental agencies as well as the design of security and incident notification requirements. An extension of the NIS principles beyond the geographic area of the EU could become a valuable contribution to a global improvement of cybersecurity in the IoT context. In particular, the IoT industry having the most advanced practical experience and know how through its human resources should start implementing cybersecurity standards based on analyses of present weaknesses, to be later followed by the involvement of intergovernmental organizations.

Security agencies all over the world need to evolve in terms of organization and investigative method with (Ruppert, Chapter 17)

> a centralized program would serve as a primary hub of all collection and investigation, thereby possessing the ability to fully comprehend the attack and facilitate the full-range response actions and preventative measures which only the whole-of-government approach has to offer. Unfortunately, such a massive shift in established bureaucratic structures to accomplish this centralization would require a level of leadership in the political structures of Washington, DC, that is unprecedented in recent history.

Along with all these changes, the enterprise system needs to continuously evolve to conform with this changing world. There will be "no shortage of new tools and services to keep any cybersecurity team busy, but it is important to not get distracted and lose focus on the human side of the cybersecurity program."

We need to "celebrate the successes, learn from the mistakes, and always remember the systems will only ever be as secure as the people who use them" (Cook, Chapter 17).

As David Thaw (University of Pittsburgh) put it,

> humans are often cited as the "weak link" in cybersecurity. While perhaps true in a highly technical sense, this claim deeply misunderstands the fundamental goals of cybersecurity, and the nature and character of the threat vectors, which will dominate the future. Rather than being the "weak link"—individuals are the purpose for which cybersecurity exists. And thus, the antiquated goal of driving humans to comply with "better security practices" must be reconsidered in light of a comprehensive approach to ensuring that information systems are designed to enable human endeavor in a manner, which effectively manages risk.

Thaw, considering the example of password complexity, believes that

> for decades, conventional wisdom recommended using complex passwords for authentication purposes. This concept originated from a 1979 paper by Morris and Thompson which demonstrated that passwords using only single-case alpha characters (26 total) were substantially more vulnerable to "key search" attacks than were more complex passwords which required more "classes" of characters (e.g., uppercase, numeric, punctuation, etc.).* For nearly 40 years following the publication of this paper, this conclusion was adopted nearly unanimously among cybersecurity practitioners.†

For Thaw

> as it turns out, this "expert" advice was wrong. Florencio, Herley, and Coskun pointed out flaws in this advice in 2007,‡ but their conclusions went largely ignored in practice until 2017. In early 2017, the National Institute of Standards and Technology reversed its position in official guidance and removed much of its recommendations for use of complex passwords to increase the security of authentication interfaces. Human factors and the additional risk vectors created by password complexity requirements were a key element of this decision.§ The lead author behind NIST's original position recommending password complexity requirements subsequently publicly repudiated the original recommendation and expressed regret about its negative impacts.¶

Thaw questions,

> How did this happen? Security is a field often driven by emotion, and the desire to feel (or help others feel) "safe." But perfect safety is an illusion. Fortunately, it is [one illusion] that society is capable of coming to terms with—as anyone who has driven (or ridden in) a car knows. Unfortunately, when it comes to cybersecurity, it is not one for which we have yet reconciled our emotions with scientific reality. Morris and Thompson's original paper did not actually counsel practitioners to require extremely complex passwords as a solution for strengthening authentication practices. It rather recommended a series of measures—most of which remain valid today—including prohibiting the use of dictionary words and specific commonly used

* R. Morris and K. Thompson, Password security: A case history, *Communications of the ACM: Operating Systems*, Vol. 22, No. 11, pp. 594–597, 1979.

† D. Thaw, Cybersecurity stovepiping, *Nebraska Law Review*, Vol. 96, No. 2, pp. 901–925, 2017.

‡ D. Florencio, C. Herley, and B. Coskun, Do strong web passwords accomplish anything?, *HOTSEC'07 Proceedings of the 2nd USENIX Workshop on Hot Topics in Security*, No. 10, 2007.

§ P. Grassi et al., Digital identity fuidelines, *National Institute of Standards and Technology Special Publication 800-63B*, 2017.

¶ R. McMillan, About those online password rules...N3v$r M1#d!—Expert who touted mixing letters, digits, symbols now regrets it," *Wall Street Journal*, August 8, 2017, p. A1.

> passwords, and the implementation of system-level security measures including guess-rate limitation and cryptographic hashing of password storage with "salting" of the cryptographic hash functions used for this purpose. Yet the most common recommendation adopted from their paper was one they did not make—requiring users to adopt and frequently change extremely complex, lengthy passwords. In other words, to provide users with a "feeling" of "taking action" to preserve their security—classic "security theater."*†
>
> To move beyond these risks, we must accomplish two goals. First, we must understand that users (humans) must actually be able to use the systems we design. Second, we must move past an emotional desire for security theater and accept that, as with any complex system, modern information technologies carry risk. There is no perfect security. But we can effectively manage risk. Moving away from rigid checklists and towards risk management plans is not only superior but necessary to a functioning society increasingly dependent on integrated information technology systems.

We will conclude this chapter with what Mohd Anwar (North Carolina A&T State University) wrote us:

> With sophisticated cybersecurity solutions, it has increasingly become hard to hack into the computer systems. Rather, new strategies to exploit human vulnerabilities are contributing regularly to successful cyberattacks. Additionally, with the rapid growth of cyber physical systems (CPS), human factor issues will be the front and center of cybersecurity. No cybersecurity solution is adequate without sound judgement and proper efforts of the human actors in the operating environment. Many times, the human actors play critical roles to deploy and operationalize cybersecurity solutions. However, the cybersecurity tasks can be impractical, time consuming, and cognitively burdensome for the human actors to perform. As a result, the human elements of cybersecurity need to be fully investigated. In essence, the cybersecurity solutions need to be usable. The usable security research should focus on answering two critical questions: (a) How humans can be assisted in carrying out cybersecurity tasks? (b) If possible, how security solutions can obviate the need of human interventions? In addition to novel cybersecurity mechanisms, this research requires understanding of the strength and limitations of human cognition and behaviors.

* B. Schneier, Beyond security theater, *New Internationalist*, November 2009.
† S. Bellovin, *Thinking Security: Stopping Next Year's Hackers*, Addison-Wesley Professional, Boston, MA, 2016.