Information & Security

Veselin Monev,
vol. 44 (2020): 27-37
https://doi.org/10.11610/isij.4403

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Cognitive Biases in the Information Security Realm: Determinants, Examples and Mitigation

Veselin Monev

ABSTRACT:

This article contributes to the theory of the human factor in the information security by explaining how bias and errors in thinking influence the perceptions and decisions in the community. Besides providing examples from practice, the author suggests recommendations for mitigating the negative effects of the cognitive biases through relevant education.

ARTICLE INFO:

RECEIVED: 09 Aug 2019
REVISED: 20 Oct 2019
ONLINE: 18 NOV 2019

KEYWORDS:

Information, security, bias, psychology, determinant, mitigation, cognitive

Introduction

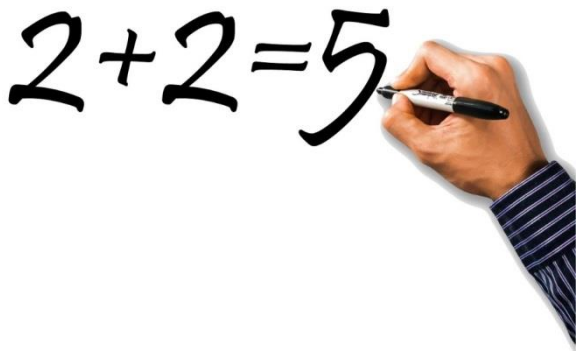
One of the components of a mature information security program is the human factor. Typically, the emphasis is on maintaining a security awareness program which aims to educate the employees about the proper behaviour when using information systems and the way to mitigate risks caused by human mistakes and lack of knowledge of security.

Security awareness is essential but it is only one aspect of the human factor. Another challenge for information security professionals from around the world, consultants, IT specialists and many others, is finding actionable and accurate arguments to support their analysis and recommendations on information security issues in their organizations. The key word here is "actionable." Their experience proves that professional logic, argumentation techniques and

E-mail: veselin.monev@gmail.com

even supporting evidences may be insufficient for managing some of the identified problems. Although a number of difficulties can be mentioned as causes for insufficient or inadequate actions on information security matters, like the lack of budget or time, lack of specialised resources, management ignorance and so forth, the picture would not be complete if the psychological phenomenon of cognitive biases is excluded.

The cognitive biases are inherent characteristics of the human nature and this way part of everyone's thinking. A bias is an error in thinking when people are processing and interpreting information and thus influencing the way they see and think about the world. Unfortunately, these biases lead to poor decisions and incorrect judgments. The reader will see that the people in the information security industry are not a special exception and can be biased like anyone else.



This article aims to contribute to the pool of information security knowledge by placing the focus on the *determinants* for cognitive biases. For this goal, the first part of the article explains several important (and non-exhaustive) determinants for cognitive biases and then exemplifies them with sample situations that can be observed in the sphere of information security. The second part gives general recommendations on how organizations can deal with the biases so that their occurrences and impact are reduced. This article does not propose a universal solution as the author believes that for each organization, unique situational solutions should be developed. The reader is also encouraged to learn about the types of cognitive biases – a topic not directly discussed here.

Cognitive biases – determinants [1] and examples

The Misperception and Misinterpretation of Random Data or Events

People deal with data on an everyday basis. The general approach when analysing data is to convert it into something more useful—information—and from there to continue the conversion into knowledge and then wisdom.[2] This complex processing chain may be impacted by the misperception or misinterpretation of random data or events. As an example, in an attempt to look for irregularities in the IDS reports, a network security professional could see random events as real attacks on a network. In this instance, the "random" data could be misinterpreted. One should understand that human's nature is inclined to look for *patterns where such do not always exist*.[3]

In a second example, a regular computer user could erroneously assume that his computer troubles are caused by malware. An experienced IT support specialist could possibly identify a different cause for the symptoms of the issue and quickly rule out the malware scenario as a cause.

Judgment by Representativeness [4]

Representativeness can be thought to have the reflexive tendency to assess the similarity of outcomes, instances, and categories on relatively salient and even superficial features, and then use these assessments of similarity as a basis of judgment.

Judgment by representativeness is often valid and helpful because objects, instances, and categories that go together often do in fact share a resemblance. However, the overapplication of representativeness is what leads to biased conclusions. Perhaps many can recall personal experiences when a person, who belongs to a certain group, is attributed qualities, considered typical for that group. For instance, some IT experts perceive the members of their information security team as very strict security and compliant enforcers but not all of them may have this profile. The stereotypical over-generalisations like "All the IT experts…," "All the auditors…," "All the consultants from that company…" often

follow imprecise and even incorrect qualifications (negative or positive). The simplification can and in some instances will be misleading.

Heading Misperceptions of Random Dispersions

If the information security specialist analyses statistical data from certain security tools, he may see patterns, which could lead him to the conclusion that certain events occur more frequently at specific time periods.[5] For instance, if a particular type of security incident occurred for four consecutive months, each time in the last five days of the month, this could indicate to him that there is a pattern. These incidents could be correlated to other known events and assumptions can be made about the underlying cause but a definite conclusion should not be drafted without additional investigation.

Solidifying the Misperceptions with Causal Theories [6]

Once a person has (mis)identified a random pattern as a "real" phenomenon, it is likely going to be integrated in the person's *pre-existing beliefs.*[7] These beliefs, furthermore, serve to bias the person's evaluation of new information in such a way that the initial belief becomes solidly entrenched. For example, if a person was the auditee during an audit several years ago where he was supposed to show to the auditor some of the IT security documents, the same person could afterwards develop erroneous expectations about future audits on different standards in another organisation. This person could be convinced that he is well aware of all the auditing practices but in reality, he could be lacking key knowledge on the specifics of other security standards and types of audits (e.g. see the difference between SOC 2, type I and type II audits).

Misunderstanding Instances of Statistical Regression

The statistics teach that when two variables are related, but imperfectly so, then extreme values on one of the variables tend to be matched by less extreme values on the other. For instance, a company's disastrous years tend to be followed by more profitable ones; Student's high scores on an exam (over 97 %) tend to follow less regressive scores in the next exam.

If people are asked to make a prediction about the next result after an extreme value, they often tend not to consider the statistical regression and make non-regressive or only minimally regressive predictions (they predict a similar value).[8] A second problem is the tendency of people to fail to recognise statistical regression when it occurs and instead "explain" the observed phenomenon with complicated and even superfluous theories. This is called regression fallacy. For instance, a lesser performance that follows a brilliant one is attributed to slacking off; A slight improvement of the security incident rate is attributed to the latest policy update; The company's IT Security Officer may be held accountable by his management for the decrease of the server compliance level after an excellent patching and hardening activity four months ago.

Misinterpretation of Incomplete and Unrepresentative Data
(Too Much from Too Little)

The Excessive Impact of Confirmatory Information

The beliefs people hold are supported mostly by positive types of evidence. In addition, a lot of the evidences are *necessary* for the beliefs to be true but they are not always *sufficient* to warrant the same. If one fails to recognize that a particular belief rests on inadequate evidences, the belief becomes an "*illusion of validity*" [9] and is considered, not a matter of opinion or values but a logical conclusion from the objective evidence that any rational person would take. The most likely reason for the excessive influence of confirmatory information is that it is easier to deal with it cognitively, compared to non-confirmatory information.

Information systems audits are good examples of *looking for confirmatory evidences*.[10] In an audit, unless a *statistical methodology* [11] is utilised for controls testing, the evidences for the effectiveness of the controls become open for interpretation and the auditor's task to perform "reasonable assurance" on the controls become as ambiguous as it sounds. Auditors would usually ask for the existence of policies, procedures and mostly look for positive evidences. Some auditors may even ignore a non-supportive evidence and ask for a supportive one. They shouldn't but they might do so.

In another example, if the security specialist in a small company has a number of responsibilities in relation to the entire information security management system (ISMS), there will be many opportunities for him to prove his abilities but also to make mistakes. If the firm's CEO favours the person, he may look for achievements that indicate his professionalism. If the CEO doesn't favour him, the focus may be on the person's past mistakes, which considered alone, would indicate incompetence. In this last case, the past successes are often ignored.

The Problem of Hidden or Absent Data

In some cases, important data could simply be absent. This makes it difficult to compare good and bad courses of action. In such cases, people could erroneously conclude that their evaluation criteria are effective. For instance, the decision to increase the level of password complexity and to lower the expiration period for the accounts of a particular business critical application represents a good security practice. However, if only this general best practice is taken into account, the expectations of the change could be overly optimistic. The reason for this is that a lot of missing information is not considered: it is nearly impossible to predict all the indirect consequences of the change, like users starting to write down their passwords and this way actually increasing the risk for password compromise.

In another example, an organisation takes the decision to outsource certain IT tasks to a third party instead of modernising the existing capabilities. This will lead to a new, perhaps better situation but there will be very limited information if that course of action is the best decision because the other opportunity will not be pursued and tested.

A third example can be given on the subject of risk assessment. People often think that if a certain risk has not occurred for years, then the likelihood for its occurrence in future is very low.[12] However, if a risk specialist thoroughly analyses the existing information on the risk, he may conclude that the likelihood of it occurring is much higher.

Self-fulfilling Prophecies [13]

A special case of the hidden data problem arises whenever our expectations lead us to act in ways that fundamentally change the world we observe. When this happens, we often accept what we observe at face value, with little consideration of how things might have been different if we had acted differently. For example, if a company's CEO believes that a member of the security team performs unsatisfactory, the last one will find it difficult to disprove him; If the CIO thinks the CISO behaves unfriendly, the last one could find it difficult to change his perception. Actually, even the absence of friendliness could be erroneously construed as unfriendliness. In such situations, the perceiver's expectations can cause the other person to behave in such a way that certain behaviours by the target person cannot be observed, making what is observed a biased and misleading indicator of what the person is like. Furthermore, if we do not like a person, we generally try to avoid him and give him little opportunity to change our expectations.

Seeing What We Expect to See [14]

The Biased Evaluation of Ambiguous and Inconsistent Data

"I'll see it when I believe it."

People are inclined to see what they expect to see and that is consistent with their pre-existing beliefs. Information that is consistent with our pre-existing beliefs is often accepted at face value, whereas evidence that contradicts it is critically scrutinised and discounted. Our beliefs may thus be less responsive than they should to the implications of new information.

For instance, if an information security consultant serves a client who is generally not satisfied with the IT services of the same company, the client may tend to scrutinise any piece of information the consultant provides to him and look for confirmations that the security consultancy services are at the same, unsatisfactory level as the IT services.

Ambiguous Information

If a decision is based on ambiguous information, we simply tend to perceive it on a way that fits our preconceptions. Why, for instance would a newly hired Information Security Officer ask questions around in his organisation? Is he not aware of his duties or is he incapable of doing his job? Is he asking questions because there is a lack of pre-existing documentation left from his predecessor? Is this what someone in this position is supposed to do? Or maybe because the ISMS can be effectively maintained only with the support and collaboration with the different roles in the organization? The answer could be related to one of these questions, a combination of them or there could be a completely different explanation. Depending on the preconceptions of each person interacting with the new Information Security Officer, they could make premature and erroneous conclusions about his capabilities.

Unambiguous Information

We tend to consider unambiguous information, which fits our beliefs, as true. However, we usually do not ignore it when it does not fit our beliefs. Rather, we try to scrutinize it and look for additional information. To exemplify this, imagine a CIO who is convinced that the employees should not be bothered with information security training and technical controls should be preferred. Then, if he is confronted with studies, which provide evidences about the benefits of persistent security awareness training, he may tend to scrutinise them and challenge the significance of the results. He may also accept with much less scrutiny other studies, which point out the benefits of technical controls over security awareness.

Mitigation of Cognitive Biases [15]

The list of determinants for cognitive biases can be extended. In any case, knowing about the problem is only the first issue. The second and more difficult challenge is to deal with the cognitive biases as effectively as possible. As far as organisations are concerned, the author suggests the creation of an entire system within the organisation, which aims to mitigate the effects of erroneous beliefs and improve employees' analytical capabilities. Depending on the characteristics of the organization, the system could be integrated in the existing training/educational program. The approach could focus on the following:

- Promoting the learning and self-improvement as a life-long process. People who embrace continuous learning and improvement will have more potential to detect their own cognitive biases and correct their erroneous beliefs. They will be also in a better position to respond on biased arguments of others.
- Promoting the benefits of scientific methods and techniques to create and test new theories with greater certainty. In addition to that, the knowledge on using scientific methods helps the people develop a mindset for structural thinking and distinguishes the critics from the closed-minded.

- Promoting and teaching argumentation techniques to improve the interpersonal skills of the employees.

Trained and motivated individuals should teach the actual techniques. The following ideas can be considered when creating such a system. Individuals can also explore most of them alone:

- When evaluating something, the various outcomes should be specified in advance. This increases the likelihood to objectively evaluate the performance of systems, processes, projects and people.
- Putting accent on the difference between generating an idea and testing it. Often, people easily create ideas but the process of proving if they work, in practice, is much more complicated.
- Organising training sessions to teach employees about logical constructs and avoiding biases.
- Distinguishing between second-hand and first-hand information and learning about the risks involved in relying on the first one.
- The benefits of using precise wording to describe and explain things and the perception risks involved when using metaphors.
- The need to focus on both – the person and the individual situation, in order to limit distortions in the perception.
- The need to understand the false consensus effect that is defined as the tendency for people's own beliefs, values, and habits to bias their estimates of how widely such views and habits are shared by others.
- The need to understand the distortions caused by the self-interest and how the organisation can refocus employees' attention to serve better its interest.
- Exploring the benefits of measurement methods.
- Learning about the tendency of optimistic self-assessments and the inclination of people to protect their beliefs.
- Learning about the benefits of focusing on both – the amount and kind of information.
- Promoting tolerance, which can be defined as the assumption that all people make mistakes. Learning about the tendency of people to remember their successes but forget their failures.
- Mastering learning techniques.
- Learning how the human brain functions from neurobiological perspective.
- Learning how to give and receive feedback. Often people hold back their own reservations and disbelief when they disagree with what someone is saying. Biased feedback leads to inability to adequately evaluate alternative strategies.

Conclusions

In a summary, this article first exemplified some determinants of cognitive biases in the context of information security and then provided several ideas how to mitigate the implications of biased thinking in the organisations. The author believes that a better understanding and awareness on the cognitive biases will be refreshing for the concept of the "human factor" in the information security industry. Most importantly, the knowledge on cognitive biases could provide a new perspective to each security process and improve communication and decision-making of individuals. As a result, the already existing set of analytical and argumentation techniques of the information security professionals could be innovatively upgraded to a new level. Such an upgrade could improve the overall well-being of the organisation, especially if it encompasses all of its members and is not limited only to the security and compliance departments.

References

1. The determinants of cognitive biases and their definitions are discussed in Thomas Gilovich, *How We Know What Isn't So: The Fallibility of Human Reason in Everyday Life* (The Free Press, 1993).
2. This is known as DIKW. See Lance Hayden, *IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data* (McGraw-Hill, 2010), 57-58.
3. The tendency of people to see patterns is discussed by Michael Shermer, "The Pattern Seeking Animal," in *How We Believe: Science, Skepticism, and the Search for God*, 2nd edition (Owl books, 2003).
4. This is related to the cognitive bias known as Representativeness Heuristic. See: Amos Tversky and Daniel Kahneman, "Judgment Under Uncertainty: Heuristics and Biases," *Science* 185, no. 4157 (1974): 1124-1131, https://doi.org/10.1126/science.185.4157.1124.
5. This phenomenon is also known as *Clustering Illusion*. It is well known among financial investors who could become overly confident when the price of a stock goes up for a couple of days in a row. See: Stephen Rogers, "Think again! Your Guide to the Cognitive Biases that Lead to Bad Investing Behaviours and the 10 Things You Can Do About Them," Whitepaper, Investment strategy group, 2017, www.investorsgroup.com/content/dam/investorsgroup/more/wp-content/themes/ig_magazine/pdf/Whitepaper_Think-again_EN.pdf.
6. The *Illusion of Causality* is a very well know phenomenon among science researchers. See: Helena Matute, Fernando Blanco, Ion Yarritu, Marcos Díaz-Lago, Miguel Vadillo, and Itxaso Barberia, "Illusions of Causality: How They Bias Our Everyday Thinking and How They Could Be Reduced," *Frontiers in Psychology* 6 (02 July 2015), 888, https://doi.org/10.3389/fpsyg.2015.00888.

7. It is also thought that pre-existing beliefs are the trigger for new beliefs. See: Michael Connors and Peter Halligan, "A Cognitive Account of Belief: A Tentative Road Map," *Frontiers in Psychology* 5 (13 February 2015), 1588, https://doi.org/10.3389/fpsyg.2014.01588.
8. Daniel Levitin, *Foundations of Cognitive Psychology: Core Readings* (A Bradford Book, 2002), 591-592.
9. The term is used by Hillel Einhorn and Robin Hogarth, "Confidence in Judgment: Persistence of the Illusion of Validity," *Psychological Review* 85, no. 5 (1978): 395-416.
10. Benjamin Luippold, Stephen Perreault, and James Wainberg, "5 Ways Auditors Can Overcome Confirmation Bias," *Babson Magazine*, February 1, 2015, https://entrepreneurship.babson.edu/5-ways-auditors-can-overcome-confirmation-bias/.
11. "Practice Advisory 2320-3: Audit Sampling," The Institute of Internal Auditors, May 2013, https://www.scribd.com/document/263463026/PA-2320-3-pdf.
12. Tversky and Kahneman, "Judgment under Uncertainty."
13. Courtney Ackerman, "Self-Fulfilling Prophecy in Psychology: 10 Examples and Definition," *PositivePsychology.com*, May 2018, https://positivepsychology.com/self-fulfilling-prophecy/.
14. Leeat Yariv, "I'll See it When I Believe it? A Simple Model of Cognitive Consistency," Cowles Foundation Discussion Paper No. 1352, 2002, https://ssrn.com/abstract=300696.
15. The application of methods to remove or reduce bias from judgment and decision making is called debiasing. Multiple other techniques for mitigating the effects of cognitive biases are discussed in "Debiasing Decisions," *Priority Systems*, 2018, https://www.prioritysystem.com/reasons1d.html.

About the Author

Veselin Monev is information security and compliance practitioner. He has over 5 years of information security experience in the academics and the private sector and more than 4 years of IT practice. In 2015 he received a master degree in Cybersecurity from the New Bulgarian University. He is author of several academic articles and co-author of an academic book for cyber security metrics.