Why Cognitive Biases and Heuristics Lead to an Under-investment in Cybersecurity

Darren Ting

1 Abstract

Because of the rapid progress in technology and data processing in recent years, technology surrounds us in the form of data, software and even smart refrigerators. With more and more companies embracing more and more complicated technology, it has led to the accessibility of more data online; however, this also results in more opportunities for this data to fall into the wrong hands. Despite the growing development in technology, companies have not placed an emphasis on its security, resulting in an increase in data breaches. This paper will discuss reasons why companies have chosen to take shortcuts and underinvest when it comes to cybersecurity through the scope of Behavioral Economics and Psychology. This will be done through an analysis of heuristics such as the Availability heuristic and biases such as the Confirmation Bias as well as how companies view risk can damage security. Then, the paper will discuss how these cognitive fallacies have affected companies, and how to improve in the future.

2 Introduction

Recently, both technology and big data are quickly becoming more and more involved within companies and businesses. According to a digital marketing study done by Smart Insights, 31% of companies have undergone a digital transformation and another 34% of companies are currently in the process of a digital transformation [4]. Thus, the integration of technology into businesses is becoming more and more frequent. The ever increasing importance of user data was highlighted in a 2014 study done by Accenture where 82% of company executives across different corporations had agreed that Big Data provides a substantial source of value to the company [2].

Many companies seem to agree that both a better integration with technology and utilization of data are important to increasing profits. Thus, these companies should value the data they obtain as well as the new technology they are developing; however, the increasing relevance of data and technology across different verticals has led to increases in attacks in the form of data and security breaches.

When breaches, whether it be security or data, occur, a company will generally not attribute the event to faulty management decisions, but rather attributed errors to technical departments; however, these mishaps may have been indirectly caused by managerial decisions that did not take security as seriously as it should have been. As a result, certain cognitive conditions that are common in psychology and behavioral economics can lead a company to becoming vulnerable to security breaches. This paper will delve into how certain psychological biases in decision making lead to weak cybersecurity among companies.

3 To The Community

In a recent podcast by the Harvard Business Review, Thomas Parenty and Jack Domet, cofounders of Archefact Group state that the current approach by organizations to cybersecurity is faulty in that it simply focuses on the technical aspects of cybersecurity. The weight of all security placed on just the IT department has had a negative impact on the cybersecurity workforce as well as magnified the gap of understanding

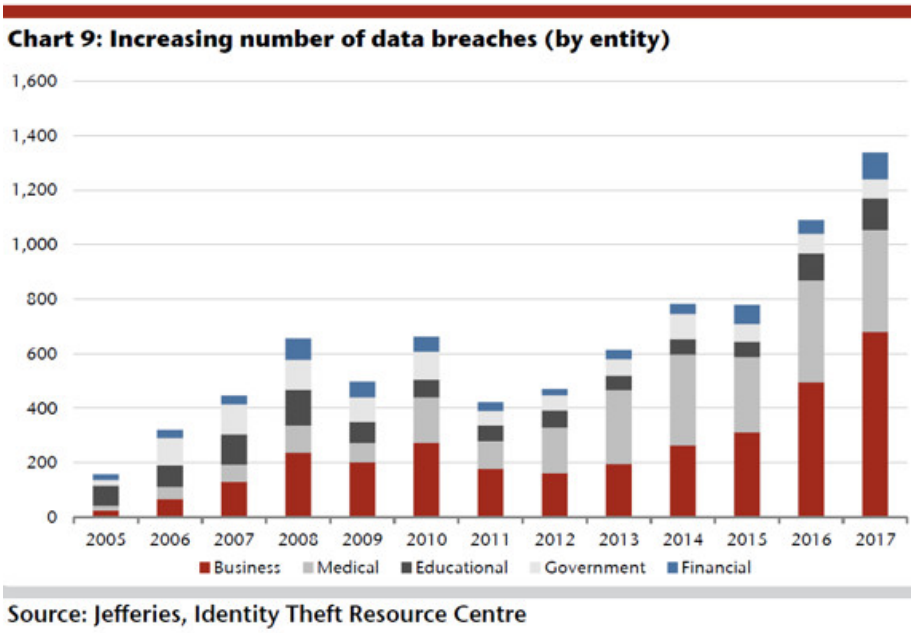

Figure 1: According to the identity Theft Resource Centre, the number of data breaches has been steadily increasing. It is important to note that this graph does not specify the number of records compromised or how much these breaches are costing businesses. These variables can also serve as metrics for how secure data in recent years.

security knowledge among cybersecurity professionals and the rest of the company. An article in 2010 lamented that the emphasis on cybersecurity training was far too low, and that there was a rising demand in the market for security employees that could not be met [7]. If there is a shortage in cybersecurity workers, it would mean that the current cybersecurity professionals now shoulder much more burden than they have been prepared for. This has resulted in considerable job fatigue that has continued to the present. Research conducted by ESG/ISSA in 2018 found that not only do 63% of cybersecurity professionals say that "cybersecurity skills shortage has increased the workload on existing staff", but also that 38% of cybersecurity professionals believe that "the cybersecurity skills shortage has led to high burnout rates and staff attrition" [17]. If these professionals are expected to do much more work with the same pay, it is almost guaranteed that there will be unhappy employees and a high attrition rate.

The clear and continuing frustration within the cybersecurity community may potentially show that perhaps a different approach needs to be made when evaluating cybersecurity decisions and that this continuing issue needs to be analyzed through different lenses. Perhaps the issue with cybersecurity does not only lie in improving the IT hiring of cybersecurity professionals but also to educate all professionals within a company about security and the faulty logic used when humans try to make decisions in regards to security without training. Understanding how cognitive biases affect decision making will spread awareness that cybersecurity is not just a technical field, and improving it will require a multitude of diverse perspectives.

4 Background Information

The ways cognitive biases and heuristics affect decision making in cybersecurity mentioned in this paper will refer to the results of the research paper *Decision-Making and Biases in Cybersecurity Capability Development: Evidence from a Simulation Game Experiment* by Mohammad S. Jalali, PH.D. The experiment consisted of a simulation game where players make investment decisions regarding cybersecurity capabilities

of a company, and then see the impact of their decisions over the course of five years within the game. The experiment had a group of cybersecurity professionals, who had worked in IT and cybersecurity for an average of 15 years [12], and a control group of inexperienced graduate students. The game itself had two levels, a deterministic level where the impacts and times were fixed, and a second level where the events occurred at random. The study keeps track of the player's profits as well as three security investment variables: prevention, detection and response. The results found that the two groups performed similarly, and that experience did not make as much an impact on performance in the game as one would expect. A closer analysis on these results will be discussed in the next section.

5 Poor Cybersecurity Decisions: Explained

5.1 Lack of Counterfactual Thinking

In cybersecurity, there is a multitude of reasons as to why a company has not been hacked yet. An executive may attribute the lack of breaches to good decision making in hiring and fund allocation; however, correlation does not always equal causation. Another view of the situation could be that they did not detect any hackers, or that they were simply lucky that year. A Harvard Business Review article attributes this type of thinking to "wrong mental models to help [decision makers] determine how much investment is necessary and where to invest...they may assume that complying with a security framework like NIST or FISMA is sufficient security" [3]. The thinking that meeting the standards of cybersecurity and then halting improvements shows that executives may view cybersecurity spending as a temporary problem as opposed to an ongoing danger. The dismissal of an absence of a breach or hack as positive result directly due to the current spending on security perpetuates an under-investment in the field.

A data breach cost study done by the Ponemon Institute revealed that in 2017, the average time it takes to detect a data breach was 206 days, which was an increase from the previous year [11]. This results in a sort of feedback delay in decision making. The study done by Jalali [12] noted that in the non-deterministic level in the game, participants struggled with adapting to the time delays especially when the time gap was significant. Unfortunately, this is closer to reality as the best hackers will not try to hack a company in a predictable fashion, and the struggle with understanding feedback delay can be seen through cognitive biases and faulty heuristics.

This delay in time between security decisions and its consequences paired with an overconfidence in security based on a lack of breaches present a dangerous combination of ignoring cybersecurity changes until it is too late. The cycle of ignoring cybersecurity by executives can be explained by the faulty logic of the availability heuristic as well as different biases such as the confirmation bias and the sample bias. The availability heuristic is a heuristic that uses examples that come to mind to evaluate a certain subject in its entirety [8]. Because of this heuristic, managers of companies that did not detect breaches in recent years may not believe the risk of hacks to be very high even though a breach may have already occurred undetected or that they simply have not been targeted yet. The lack of counterfactual thinking by managers and executives due to a lack of breaches is aggravated by the confirmation bias, which is a tendency for an individual to interpret events in a way that confirms that individual's beliefs [8]. As a result, an absence of detected breaches and vulnerabilities could confirm an executive's belief that his or her company is secure, thus believing that correlation is causation. Another bias exasperating this belief is the sample bias. The sample bias essentially is one seen in studies and in statistical analyses: a poor sample size or sample choice will skew the results to a non accurate conclusion [10]. If a company executive bases security spending decisions based on a small sample size made up of companies following similar standards as well as the security breaches on the news, then the decision may not be made based on accurate data. A potential explanation for the increase in breaches recently could be that many executives in previous years did not invest enough in cybersecurity because of the lack of breaches on the news and among peers. Through the unpredictable feedback delay, this lack of investment across different companies resulted in a weaker cybersecurity that is now being exploited by hackers leading to a substantial increase in security breaches. While this is simply a claim, it does highlight a danger in the way executives have approached cybersecurity

in the past, and how decision making in security is psychologically difficult.

The performance of security decision making against delayed feedback in the study is not only seen reflected through the increase in breaches, but also explained by the many biases plaguing human decision making. The indifference in results across experience in the study shows that not only is decision making in cybersecurity is unnatural to the way human brains function, but also that a lack of negative cybersecurity activity clouds judgement through the different cognitive fallacies implanted within human thinking. Therefore, more attention needs to be consistently shown to cybersecurity and how a company deals with cybersecurity risks.

5.2 Risk Mitigation vs Risk Management

Weaknesses in security and vulnerabilities are viewed as risks. Security requires trade-offs in that by investing more in security, a company misses out on potential profit; consequently, it is impossible to be both a feasible, profitable company and have perfect security. Inevitably, companies will have security that need to be managed through a preparation of responses to said risks. In the study done by Jalali, runs of the simulations can be divided into two types: proactive and reactive. [12].

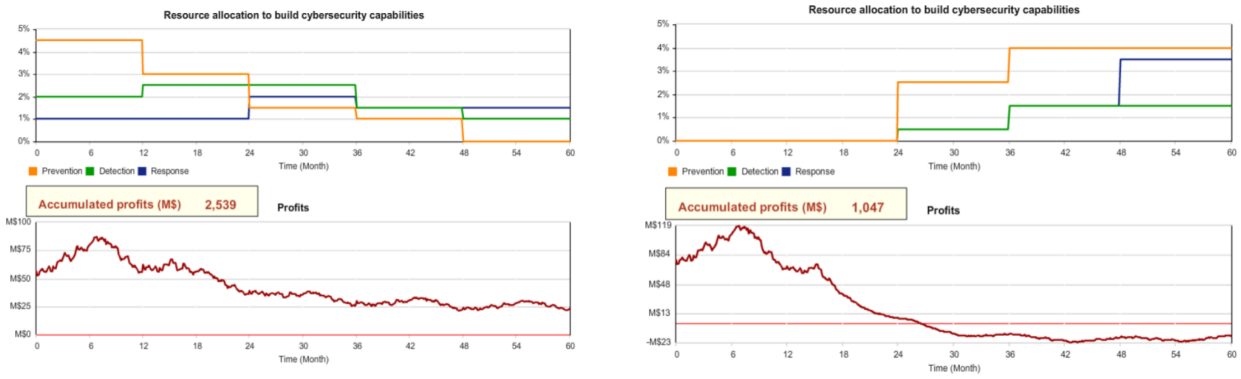

Figure 2: These graphs from the study have three variables, prevention in orange, detection in green and response in blue, The graph on the left represents a proactive run, while the graph on the right is reactive [12]. In proactive runs, a player invests in the three variables early on and make lower profits in the beginning; however, a proactive player will sustain profits in the long run. A reactive player makes more profit in the beginning because he or she will not invest in security capabilities at all. These players would then start losing money because of the attacks. Profit, pictured on the bottom of each graph, is measured over months and is shown in millions of dollars

Worryingly, the results of the study found that the professional subjects do not act more proactively than inexperienced subjects. In addition, under "Limitations and future related directions", the author states that "observations show that many organizations that develop cybersecurity capabilities seem to take prevention and detection capabilities into consideration while ignoring response capabilities" [12]. This highlights the issue that cybersecurity professionals tend to focus too much on risk mitigation when risk management through response is equally important. In the Harvard Business Review article mentioned before, the vice president of a behavioral science consulting firm states that cybersecurity has been treated "as a finite problem that can be solved, rather than as the ongoing process that it is. No matter how fortified a firm may be, hackers, much like water, will find the cracks in the wall" [3].

The bias towards focusing on prevention and risk mitigation can be explained by the zero risk bias. Within psychology, zero risk bias is defined by the tendency to prefer the value of certainty and opt for zero-risk solutions [19], even if this results in a less favorable outcome. The idea of preventing security breaches seems more appealing because it almost implies that breaches would be impossible when prevention is done

correctly. It remains a pessimistic truth that vulnerabilities are inevitable, but it is one that executives must understand in order to manage risk and lower the chances of expensive breaches occurring. The absence in risk management paired with innovation can aggravate the damage it can cost to users, as seen in the example of a certain new technology.

5.3 Pro-Innovation Bias and the Bandwagon Effect

IoT (Internet of Things) is a technology now quickly catching the eyes of countless businesses, with its usage in businesses growing from 13% in 2014 to 25% today as well as a worldwide device number projected to be at 43 billion by 2023 [9]. While the potential this technology has is significant, it also has clear issues.

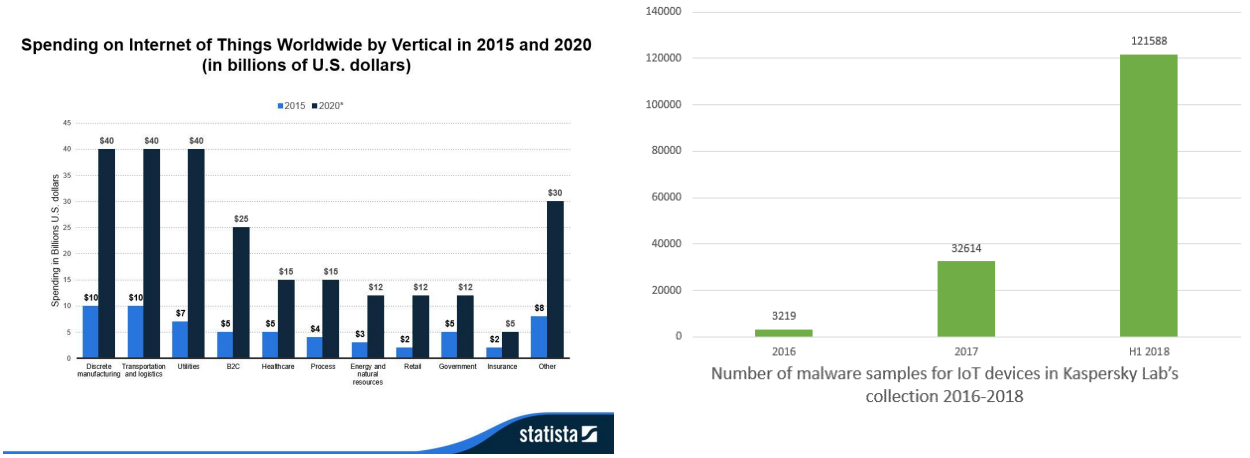

Figure 3: The graph on the top left, a Forbes article in 2017[6], shows the increase in spending in IoT technology between 2015 and 2020 (projected). The increase in investment reveals a clear global interest in the technology. The figure on the right shows the exponential increase in malware samples in IoT devices from 2016 to 2018 where 121,588 samples of Malware were found by one antivirus software alone. [20]

Like many other investors in new technology, many of the ones that invest in IoT are affected by not only the Bandwagon effect as well as Pro-Innovation Bias. The Bandwagon effect is one where the rate of belief and confidence in new ideas, or in this case, technologies, increases more rapidly as the number of believers increase [5]. This effect is generally used to explain trends [13], or the idea of people supporting an idea simply because it is popular. While in something like fashion, there may not be drawbacks to trends coming and going; however, this is not the case in technology as it may be integrated into daily life and potentially lead to harm. This harm can occur in the form of the Pro-Innovation Bias which leads the to belief that an innovation should be adopted by society as a whole without any sort of changes [18]. In terms of technology, this cognitive bias affects business decision making in how quickly companies proceed in developing insecure technology.

In 2015, the FBI released an article warning consumers about how insecure IoT technology is and how criminals can exploit vulnerabilities within it [1]. Nevertheless, a casino was hacked in 2016 through one of its fish tanks that was connected to the casino's network [14]. Through the Bandwagon effect, the clear vulnerabilities in IoT technology are ignored while the potential benefits are prioritized. Because of its rising popularity, investors, enthusiasts, and companies hoping to produce IoT software while the popularity still surges are susceptible to pro-innovation bias, which will further downplay the glaring weaknesses that IoT technology has, setting up easy targets for malicious agents. In this case, IoT is used as an example of a market that has insufficient security due to cognitive bias among consumers which means to say that it may not be the only one.

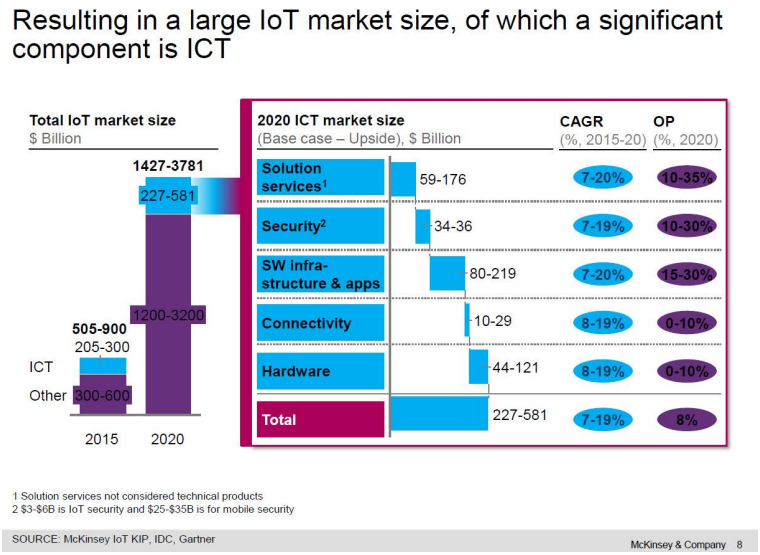

Figure 4: This graph depicts the components of IoT's market spending [6], and shows that security of IoT products is the 2nd lowest in fund allocation.

6 Action Items

Since cybersecurity is an ongoing issue a company must manage, there is always a chance for improvement. Many of the issues mentioned here stem from cognitive errors in evaluating information and the resulting decisions made. Awareness of the existence of these cognitive biases can be a first step to avoiding them. An article in the Cybersecurity Review suggests that teaching employees about cognitive biases and logical constructs, learning how to take and receive feedback, and evaluating information objectively are some ways to combat cognitive bias [16].

Changing the current perspective on cyber risks would also somewhat alleviate the issues stated in this paper. An article written by a former senior advisor for public affairs at the Department of Homeland Security not only called for viewing cybersecurity as not just a technical issue, but also compared it to disease management in that it "requires ongoing care, not one-time intervention" [15]. By viewing cybersecurity as a risk management process instead of a risk mitigation process, it can pave the way to better responses to breaches.

In the study done by Jalali, he states that "behavioral economics research shows that managers rely on a set of heuristics to make decisions in situations with uncertainty, and that these heuristics can potentially cause systematic errors. This phenomenon has received little attention in cybersecurity research, which is concerning, as a manager's biased assessment of cyber risks could hamper an organization's ability to respond to cyberattacks" [12]. The growing importance of cybersecurity needs to be met with a growing number of different approaches to improving security, one being through a behavioral lens. Thus, the concern mentioned in the study should be brought to light, and more studies on optimal decision making in cybersecurity need to be done.

7 Conclusion

Because technology has become more omnipresent, the understanding of its security needs to be just as important in more than just technological roles. Faults in a company's security, in the form of breaches, are attributed to technical vulnerabilities; however, security issues can stem from the executives making decisions revolving around allocation of funds. Since humans are making these choices, cognitive biases must be taken

into account. These biases have led to a lack of counter-factual thinking as well as a view of cybersecurity as a problem to be solved, not a risk to be managed. People need to be more wary of new technology and its undiscovered vulnerabilities before believing in its potential as to combat the bandwagon effect and pro innovation bias. Approaching the field of cybersecurity through different lenses, including a behavior one, is vital to its future in order to grow and thrive.

References

[1] Cyber tip: Be vigilant with your internet of things (iot) devices. *FBI*, 2015.

[2] Accenture Analytics. Companies are satisfied with business outcomes from big data and recognize big data as very important to their, Sep 2014.

[3] Alex Blau. The behavioral economics of why executives underinvest in cybersecurity, Aug 2019.

[4] Dave Chaffey. How many businesses have a digital transformation programme in place? 2019.

[5] Andrew Colman. Oxford dictionary of psychology. *New York: Oxford University Press*, page 77, 2003.

[6] Louis Columbus. 10 charts that will challenge your perspective of iot's growth, Jun 2018.

[7] Mike Cronin. Universities push to turn out cyber guards as demand explodes, September 2010.

[8] Steve Dale. Heuristics and biases: The science of decision-making. *Sage Journals*, 2015.

[9] Alexander Rajko Fredrik Dahlqvist, Mark Patel and Jonathan Shulman. Growing opportunities in the internet of things, July 2019.

[10] Farlex Inc. Sample bias, 2011.

[11] Luke Irwin. How long does it take to detect a cyber attack?, Mar 2019.

[12] Mohammad S. Jalali, Michael D. Siegel, and Stuart E. Madnick. Decision making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *CoRR*, abs/1707.01031, 2017.

[13] D. Stephen Long, Nancy Ruth. Fox, and Tripp York. *Calculated futures: theology, ethics, and economics*. Baylor University Press, 2007.

[14] Lee Matthews. Criminals hacked a fish tank to steal data from a casino, July 2017.

[15] Gregory Michaelidis. The road to cybersecurity is paved with "extraordinarily basic things", Apr 2018.

[16] Veselin Monev. Cognitive biases in information security causes, examples and mitigation, Aug 2018.

[17] Jon Oltsik. Cybersecurity job fatigue affects many security professionals, Feb 2018.

[18] Everett M. Rogers. *Diffusion of Innovations, 4th Edition*. Free Press, 1995.

[19] Elisabeth Schneider, Bernhard Streicher, Eva Lermer, Rainer Sachs, and Dieter Frey. Measuring the zero-risk bias. *Zeitschrift für Psychologie*, 225(1):31–44, 2017.

[20] Al Smith. The vulnerability of iot cybersecurity - dzone security, Jan 2019.