Human Behavior Is a Significant Flaw In Maintaining Cyber Security

Elizabeth Jackson

Old Dominion University

July 30, 2020

Abstract

Human behavior and data security utilization must be intertwined; in order to mitigate the negative effects of cyber attacks. No consumer wants their data hacked, breached, stolen, shared or wiped out. It is imperative to survey the type of education is needed to keep users safe and interested in securing their data. This can be done by simply seeking out the consumer's view of data security. The information obtained would allow the cybersecurity community to offer a simple way for consumers to protect their mobile data. There is a constant interaction between human behavior and the need for increased data encryption. Because technology increases convenience to the human experience; there will always be a point where the fine line between the two poses a significant risk to providing adequate cybersecurity.

Humanity's emotional involvement in this complex process leads to outcomes that do not reflect the need for optimized data encryption. Thus there is an inherent need to practice logic and pragmatism in decision making regarding when to protect it and ultimately how to protect one's data. Having total protection along with overall security is deemed impractical due. The dilemma is always how much security is too much and how much opened data is too much. This is an individual question that most of us struggle with in today's environment. The most secure storage device is a rock, but it does not share data very efficiently.

That does not mean that optimal data protection (freedom of use and encrypted use) cannot be achieved; without regard to emotive decision making. The objective of this paper is to identify how human behavior is one of the greatest contributing factors is human behavior contributing to the lack of security. My focus will be narrowed down to weaknesses that occur due to inadequate cell phone data encryption methods being used. The lapse in data security lends the wireless community vulnerable to critical data breaches. These breaches permit threats that affect corporations, communities, and end users on a global scale. Where there is a lapse in data encryption there is also an exploitable loophole for malware and hackers.

Introduction

The desire for advancements in technology have a direct correlation to humanity’s need for convenient data dependency. The more dependent mankind becomes on technological advancements; the more data security becomes compromised. Technology is an evolutionary process full of new advancements and intricate systems. The epicenter of every cyber system requires human interaction to constantly cultivate encryption through an evolution of peak efficacy. This is a huge undertaking without end user cooperation.

There are numerous underlying issues when it comes to maintaining security. For instance, not understanding operating systems of cell phones and inadequate security measures to secure the phone/data. Security measures could be different passwords, knowing how to

evaluate a threat and implement the necessary steps to prevent exposure. The most pertinent one being human behavior toward technology is a minimal priority in today's cybersecurity platforms.

Human behavior does predict the effectiveness of security systems, however encryption is only as good as the end users' confidence in the importance of utilizing it. This factor ties into every security measure due to the fact that security is reliant on the responsiveness of the user. These tasks can only be done if the individual recognizes and trust measures that've been put in place. For the purposes of this study we will look at the computing devices most commonly used by mankind without regard to encryption level security; cell phones. The consumer and the regulating agencies set in motion an incentive to provide secure set up, login and data protection protocols across all operating systems platforms to combat human deficiencies.

Weakness linking human behavior to cyber defense

It's pretty hard to come across someone who doesn't own a cell phone in the United States. Having a cell phone is very much a mini computer considering all its capabilities. There is more computing power in one cell phone than we had on any Apollo capsules to the moon. Cell phones provide numerous ways of linking everyday activities or aspects of people's lives. With an individual's life being more connected to various types of technology and data; it is important to have a data security plan. Because cellphones are used as a common data resource, consumers become complacent with sharing and receiving massive amounts of data. The frequency with which data is transmitted and received, creates opportunities for data breaches due to failure to check the security of information sent/received. The sharing and storing of data while not knowing the integrity of your security plan leaves vulnerabilities to data breaches and hacks.

The transparency and efficiency of security systems built into cellphones are weakened by consumer behavior. Some examples of this are; using obsolete security methods, downloading malicious apps, jailbreaking the device, opening emails/texts with unknown links or seemingly familiar content. Human error can be placed into two different types: skill-based and decision based errors. Skill-based human error consists of slips and lapses: small mistakes that occur when performing familiar tasks and activities (Ahola, 2019). This type of error refers to individuals who already have the experience and knowledge to complete or make an action correctly. Having their focus directed elsewhere, to aspects of the environment around them and personal thoughts/problems can sway a person into making errors. Decision-based errors are when a user makes a faulty decision (Ahola, 2019).

Given everyday interactions whether it's dealing with work, personal info, etc it's easy to lose sight of how much information the individual is sharing or how an action can cause careless lapses in data security. The line of oversharing and knowing when to withhold certain information is critical. Because most individuals lack the training and understanding to secure their devices and its data contents, they resort to inaction, as a matter of conveinence. The tendency to take the simplest route or find even the slightest shortcut to make the security

process less of a hassle is detrimental to the security of cellphone data. The effect of this behavior is a mitigation of the security plans overall goal of keeping information secure. To maintain transparency in data security, the creator and end user must follow the same protocols to protect the information as it is transmitted.

The potential extent of the human behaviors

In cybercrime, the methods hackers use are often only as successful as the users willingness to open unsolicited data packages. These can be; emails, website links, application advertising, text messages and, other common data sharing platforms like messenger, snapchat, etc. Some methods to infect cell phones will use these entry points to ask for permission to use photos, phones, location, data, account information, and many other items. If the consumer is not paying attention they will agree to this use of data and unwittingly volunteer data throughout their cellphone's system. With cybercrime the methods hackers use often are only successful when the user behavior falls for misleading tactics. These tactics allow the introduction of malware to the consumers cellphone.

Exposure to malware can result in data being stolen and damaged in the process. One of the more common ways that data security is breached is through accessing unsecured wifi networks and outdated operating systems. According to consumer groups, about 40% of Android users were running older versions of the software, which no longer received security updates from google (Griffin, 2020). This can lead to data being shared with third parties or again the device could be exposed to malware. These exposures come as a result of devices not having the latest defense against constantly evolving hacking programs. Another way outdated operating systems are vulnerable is; malware may have access to older updates to block newer updates from being downloaded if too many updates are ignored. These are just some of the ways an individual can find themselves susceptible to security risk.

Data protection education is a key component in strong cell phone security

When consumers receive education on the many aspects of why a security protocol is in place it makes it easier for them to want to comply with the process. Increasing education on data security will improve the chances of end user compliance with security measures. Data protection courses could be offered as a starting point; for anybody is several strong passwords, and to include a two factor authentication as a requirement. The two factor approach is an extra layer of protection by not only using a username and password, but utilizing questions, biometrics (ex: fingerprint), and push notification authentication. Individuals tend to put these unique passwords on a piece of paper or in a "password book" , thus leaving a hard copy of their information. When dealing with sensitive data there needs to be education on how and where to store passwords. Teaching consumers to use password encryption programs would help users control access to data.

Data education on software and security updates would also be a positive factor for the end user. Instead of putting off a software update that seems like an inconvenience, it should be

installed as soon as it's available because it lessens the risk of being compromised. The software updates are typically to address data security issues within cell phones systems. Encrypting any sensitive data on the mobile device, ensures it remains intact by having an additional layer of protection even if it's stolen. Phones have a security in place to act as an antivirus, installing firewalls for the devices data. Education on what happens when a consumer jailbreaks a device is vital to data security. When an individual jailbreaks their cell phone they're removing software restrictions allowing access to the root of the operating system. It also gives the user the ability to install & use unauthorized applications to be downloaded to the phone. The process of jailbreaking is basically putting the whole system at risk by stripping away the built-in security.

Unsecured networks typically don't require login information and allow use as long as the user is in range. So when using these types of networks it's important to avoid access to any form of personal information whether its bank account, documents, or making an online purchase. Teaching the consumer to take a second glance at websites can help them with remaining on secure sites; as a matter of habit. For the purposes of finding out the extent to which consumers would benefit from the aforementioned data education program for cell phones; a survey will be created. The survey will pose questions to the consumer that help give a picture of areas where education may be a bridge between end user behavior and security platform integrity.

The questions posed and the offered responses are included here:

1. Do you store sensitive information on your device?
    a. Yes
    b. No
2. If you received an email asking for information do you respond?
    a. Yes
    b. No
3. Do you click/open links that you received via email or text?
    a. Yes
    b. No
4. When you receive a random text and the number seems familiar to someone you know, how do you respond?
    a. I don't at all
    b. Block the number
    c. Ask who is it
    d. Open the text and see where it leads

5. Do you accept the terms of apps or websites? For example snapchat, facebook, fitness apps, tiktok, etc..?
    a. Yes
    b. No

6. Before accepting these terms do you read the fine print?
    a. Yes, I read the terms thoroughly
    b. Yes, I skim through it
    c. No, but I read the initial statements before I accept
    d. No, there too many pages
7. Do you have protection on your device?
    a. Yes
    b. No
8. If so, how do you protect your device? (click all that may apply)
    a. Difficult password
    b. Security software
    c. Remote data wipe
    d. location tracking
9. There's a new operating system update for your device, when do you install it?
    a. When it's a convenient time
    b. Immediately
    c. Never
    d. Every once and awhile
10. Do you link home gadgets like security systems, amazon alexa, etc..linked to your cell phone?
    a. Yes
    b. No

11. Do you permanently delete apps and files from your device?
    a. Yes
    b. No
12. How often do you rid your phone of apps and files you do use or need?
    a. Every once and awhile
    b. Every 6 months
    c. Right when i'm done using it
    d. Sometimes, but I mostly save them for later use

13. Do you have apps like google drive, dropbox, onedrive to store all your files?
    a. Yes
    b. no
14. How do you protect your files stored on your phone?
    a. Store and save them in a app on my phone
    b. Encrypt the files
    c. I don't store them on phone
15. Do you open documents from various search engines?
    a. Yes
    b. No

With these questions a weight for each answer and the percentage of survey participants that gave the answer would be reviewed and weighed to determine four things. Is there evidence of consumer security conscientiousness, ie. "I pay attention to what happens to my information." Is there complacency in the users attitude toward data protection; ie. "It would never happen to me." Do the survey participants answer toward more security education, ie. " If I knew how to secure my data I would." or Do the survey participants answer toward more convenience than security, ie. "If I have to choose between getting the information I want immediately or learning to get it in a secure manner a little slower; I would rather risk the hack."

Conclusion

An education application/survey could be added to the set up of a cell phone to require the user to demonstrate or take a short security education training for their device. Based on the survey questions an appropriate security application can be installed and taught to the consumer. This would mitigate some of the startling findings about inadequate data security. The National Cyber Security Centre states that almost half (46%) agree that most information about how to be secure online is confusing, though this falls to 18% who agree strongly (ncsc.gov, 2019). It's an opportunity to assess weaknesses and strengths of the users' understanding regarding the security of their data.

Educating on security practices is a vital approach because an individual who gets the basic security practices will know how to avoid issues. Which will help reduce the number of human errors when handling data. The same application/survey could also allow the user to disagree and waive their right to secure data transmission and reception on their cell phone. With these choices the user is then taking responsibility for making their data more secure or the resulting risk of not obtaining the knowledge to protect their information.

If security awareness was normalized, an individual would be prepared and knowledgeable about the preventive measures needed to maintain security. The survey could be a stepping stone to solidify where the focus needs to be, which is human behavior. This also allows cell phone developers to see where human error causes data security lapses and connects them with the

mindset of the individual. Identifying what an individual's thought process or course of action is when dealing with the various scenarios, like the ones presented in the questions above.

References

A. (2018, December 3). Human Behavior the Weak Link in Cyber Defense. Retrieved June 27, 2020, from https://www.apacciooutlook.com/news/human-behavior-the-weak-link-in-cyber-defense-nwid-5431.html

Ahola, M. (2019, October 18). The Role of Human Error in Successful Cyber Security Breaches. Retrieved July 4, 2020, from https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches

Capone, J. (2018, May 25). The impact of human behavior on security. Retrieved May 3, 2020, from https://www.csoonline.com/article/3275930/the-impact-of-human-behavior-on-security.html

Cosgrove, A. (2019, February 27). Human behavior can be your biggest cybersecurity risk. Retrieved June 9, 2020, from https://www.helpnetsecurity.com/2019/03/04/human-behavior-cybersecurity-risk/

Ghosemajumder, S. (2017, December 04). You Can't Secure 100% of Your Data 100% of the Time. Retrieved August 14, 2020, from https://hbr.org/2017/12/you-cant-secure-100-of-your-data-100-of-the-time

Griffin, A. (2020, March 06). More than a billion Android phones are now at risk of being hacked, experts say. Retrieved July 9, 2020, from https://www.independent.co.uk/life-style/gadgets-and-tech/news/android-phone-hack-update-software-operating-system-warning-a9383716.html

Hackers Attack Every 39 Seconds. (2020, May 24). Retrieved June 15, 2020, from https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds

N. (2019, April 21). Most hacked passwords revealed as UK cyber survey exposes gaps in online security. Retrieved April 21, 2020, from https://www.ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security

Page, D. (n.d.). 5 Ways Your Mobile Device Can Get Malware. Retrieved July 22, 2020, from https://www.securitymetrics.com/blog/5-ways-your-mobile-device-can-get-malware

Stanley, J. (2017, September 7). Guard Your Privacy. Retrieved July 11, 2020, from https://www.timeforkids.com/g34/guard-your-privacy/