International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 04 | Apr 2021 www.irjet.net p-ISSN: 2395-0072

Is human error paving way to Cyber Security?

Menon Sanoop Govindankutty

Student, M.Sc IT, Keraleeya Samajam (Regd.) Dombivli's Model College, Maharashtra, India

---

Abstract - *Cyber Security one of the hot topic and a serious concern. In this digital world almost every department are now dependent on IT infrastructure and their security is a big concern. Organizations and individuals invest a big amount for the security. Despite overall increase in cyber security investment over the past decade by multinational companies and organizations the security breaches are explored by the attackers due to human mistakes. Human error are one of the vulnerability which are used by the attackers. As per some studies human error are the main cause of cyber security breaches. The following paper is regarding how human error a breach to cyber security.*

Key Words: Cyber Security, IT, Human factor, Data breach, Social engineering.

1. INTRODUCTION

Securing network has now become a big concern of any organization. Cyber attacks are increasing day by day. There are many methods to make a system malicious and get into the system and to steal authenticated data from the system. Organizations and individuals invest on cyber security to stay away from such attacks by using updated antivirus and antispyware, using firewall, up to date updates of operating system and many for technologies. But the main breach which the attackers always try to exploit is human error.

There are mainly 2 types of attacks which is Passive attack and Active attack. Passive attack is a method where a attacker just monitor but they do not make any changes in data. Active attack is a attack where the attacker tries to modify the content of the data.

Human error means a unintentional actions occurred by the individual which make a loophole or breach through which an attacker can access the system.

There are many ways an attacker can force human to make mistakes. One of the main attacks against human is social engineering

The attackers try various methods to find loophole in the system as a gateway to get into the victim system and access try to gain unauthorized access to confidential data. There are various range of action by which the attacker can get in to system by human mistakes that may be the malicious infected attachment to weak or easy guessing passwords.

With more investment in IT infrastructure more advanced technologies are introduced to the humans, various multiple. tools are used for which users have to use username and password to secure the tool. For each tools there will be a username and password to get the access of the tool, so the humans have to remember the username and password for each tool they use, which is little complicated. Remembering more than multiple username and password is little difficult, so employees or individuals start taking short cut to make life easier, use same credential for multiple logins or save the credentials or note it down somewhere they remember, which opens a gateway for the attackers.

[1] Social engineering is the art of exploiting human psychology, rather than technical hacking techniques, to gain access to buildings, systems or data. It is one of the effective method to exploit human errors. For example the social engineer will not try to exploit the software vulnerability instead they try to trick the employees or individuals to gain credentials .

There are infinite number of opportunities for human error, they can broadly divided into skill-based and decision-based error. Skill-based error are something which occur due to tired, not paying attention and distraction while performing familiar tasks and activities. Decision-based error are something which occur due to the user dose not have the information for specific circumstance or necessary level of knowledge.

2. DATA BREACHES CAUSED BY HUMAN ERROR.

[2] 2.1 Equifax — Expired certificates delayed breach detection

In the spring of 2017, the U.S. Department of Homeland Security's Computer Emergency Readiness Team (CERT) sent consumer credit reporting agency Equifax a notice about a vulnerability affecting certain versions of Apache Struts. According to former CEO Richard Smith, Equifax sent out a mass internal email about the flaw. The company's IT security team should have used this email to fix the vulnerability, according to Smith's testimony before the House Energy and Commerce Committee. But that didn't happen. An automatic scan several days later also failed to identify the vulnerable version of Apache Struts. Plus, the device inspecting encrypted traffic was misconfigured because of a digital certificate that had expired ten months previously. Together, these oversights enabled a digital attacker to crack into Equifax's system in mid-May and maintain their access until the end of July.

[2] 2.2 Ericsson — mobile services go dark when the certificate expires

At the beginning of December 2018, a digital certificate used by Swedish multinational networking and telecommunications company Ericsson for its SGSN–MME (Serving GPRS Support Node—Mobility Management Entity) software expired. This incident caused outages for customers of various UK mobile carriers including O2, GiffGaff, and Lyca Mobile. As a result, a total of 32 million people in the United Kingdom alone lost access to 4G and SMS on 6 December. Beyond the United Kingdom, the outage reached 11 countries including Japan.

[2] 2.3 Veeam — Customer records compromised by unprotected database

Near the end of August 2018, the Shodan search engine indexed an Amazon-hosted IP. Bob Diachenko, director of cyber risk research at Hacken.io, came across the IP on 5 September and quickly determined that the IP resolved to a database left unprotected by the lack of a password. The exposed database contained 200 gigabytes worth of data belonging to Veeam, a backup and data recovery company. Among that data were customer records including names, email addresses and some IP addresses.

[2] 2.4 Marine Corps — unencrypted email misfires

At the beginning of 2018, the Defense Travel System (DTS) of the United States Department of Defense (DOD) sent out an unencrypted email with an attachment to the wrong distribution list. The email, which the DTS sent within the usmc.mil official unclassified Marine domain but also to some civilian accounts, exposed the personal information of approximately 21,500 Marines, sailors and civilians. Per Marine Corp Times, the data included victims' bank account numbers, truncated Social Security Numbers and emergency contact information.

[2]2.5 Pennsylvania Department of Education — misassigned permissions

In February 2018, an employee in Pennsylvania's Office of Administration committed an error that subsequently affected the state's Teacher Information Management System (TIMS). As reported by PennLive, the incident temporarily enabled individuals who logged into TIMS to access personal information belonging to other users including teachers, school districts and Department of Education staff. In all, the security event is believed to have affected as many as 360,000 current and retired teachers.

3. HUMAN ERROR IS TO BLAME FOR BREACHES ?

Each year every company invest in new cyber security technologies, and attackers try to break that technologies with new tactics and tricks. Organizations and individuals put so much efforts for securing the system and still the attacks occur and while tracing the breaches it is commonly seen that majority of the breaches are occurred due to human mistakes.

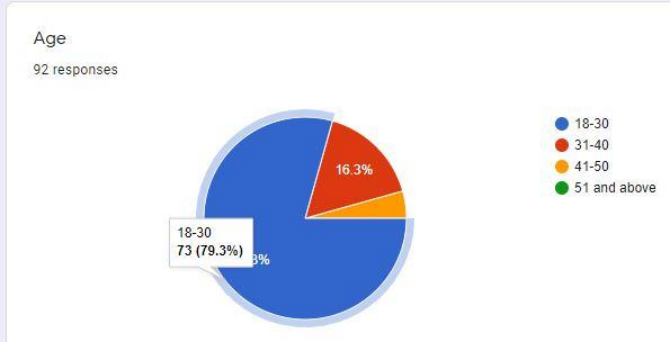
According to Will R. Daugherty[3] Human error as the leading cause of incidents 37%, followed by phishing/malware 25%, external theft of a device 22%, and employee theft 16%.

Attackers are increasingly relying on phishing attacks, emails, calls texts to trap humans. They send malicious link with the mails and text and humans click the link unknowingly what inside the link and allowing the attackers to get into system.

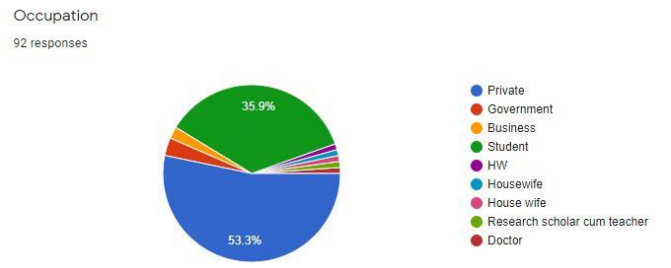
External theft is also occurs due to the human error. Leaving laptop and mobiles without locking the system, in unlocked cars and in unsecure places. Internal theft is something which occurs inside the organization accessing the documents, devices containing sensitive data by the employee who is restricted to access the sensitive data or someone was authorized to access the data but after the employee is resigned or terminated still he/she has the access to the sensitive data. Shoulder surfing is another attacks occurs in offices, public places where the user inputs credentials details and someone observe the details capture the details without users permission.

4. SURVEY

This survey is conducted by me on few people about regarding some general information. Following is the result of the survey

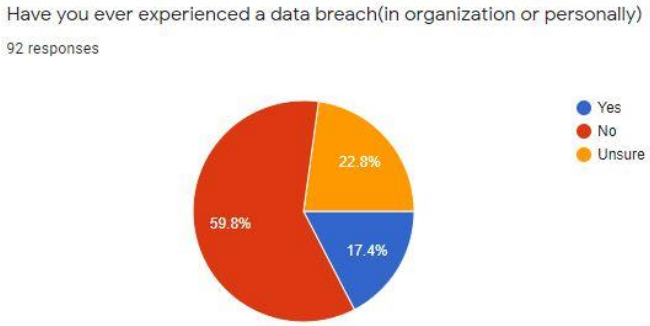


18-30 is the age group filled my questioner most 79.3% and the other age group is 31-40 16.3% and 41-50 4.3% who filled the survey questioner. So total of 92 responses I got from this survey.

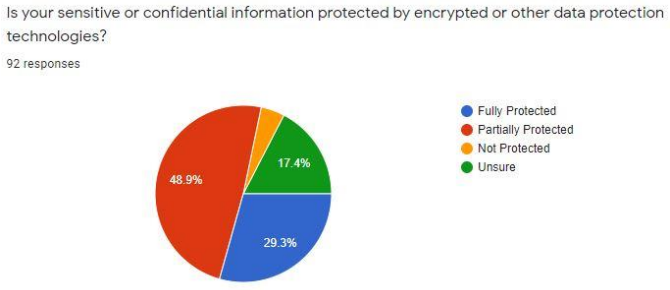


From 92 responses 53.3% are working in private organizations and next majority who filled the form is students 35.9%.

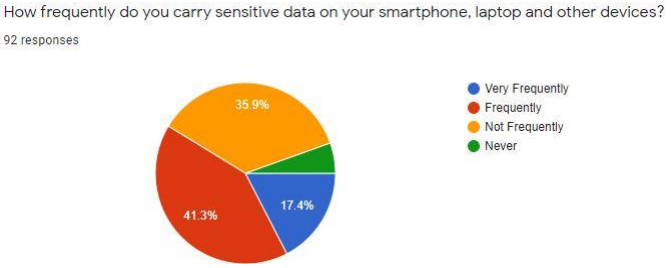
From 92 responses 34.8% given 3 out of 5, and 31.5% have rated 4 out of 5, only 8.7% are rated 5 out of 5, 2.2% are not aware about what cyber security is.



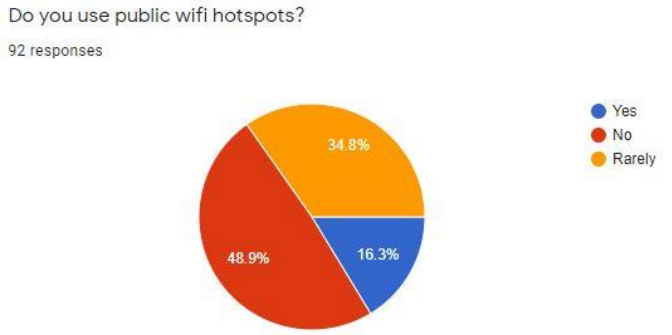
59.8% have not faced any data breach from my survey but 17.4% people have faced the data breach and remaining 22.8% are not aware about whether they have experienced the data breach.



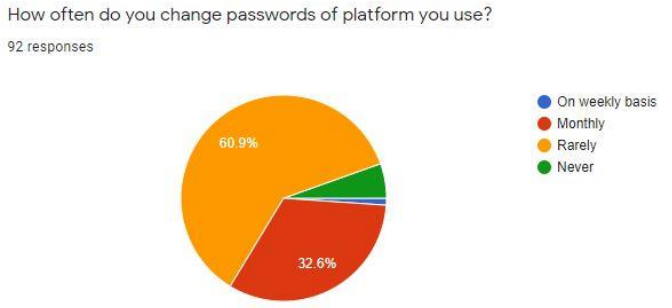
This question was intended to know about whether their sensitive and confidential information is protected by encrypted or other data protection technologies. The response was 48.9% of them says their confidential data is only partially protected, 29.3% of them only says their data is fully protected, but 17.4% says they are unsure about their data is protected or not which is a major issue and 4.3% says their data is not protected.



From the above graph 17.4% Very frequently carry sensitive data and 41.3% carry frequently, here the chance of external theft is very much possible, attackers may observe the movement and plan accordingly to the situation.35.9% says they do not carry data frequently and only 5.4% do not carry any sensitive and confidential data.

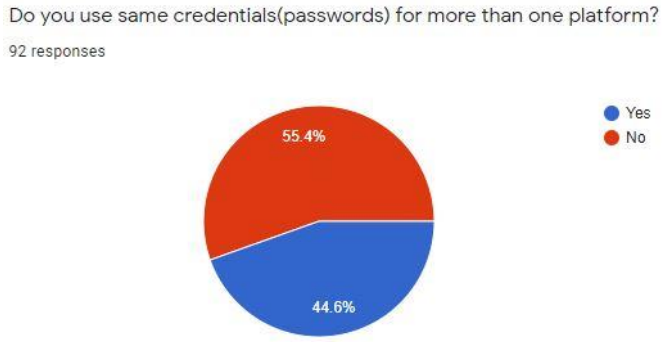


By this question I want to know that how many of them connect to the public wifi hotspots and in response 48.9% says they do not connect to public wifi hotspot, 34.8% says they rarely connect and 16.3% says they connect. It has been observed that attackers are hacking the people who connect. Free public wifi is available in lot of places- Railway station, Airports, Shopping malls, Hotels, Bus stand etc. One of the attack occurs in public wifi is man in the middle attack. When attempting to use the public wifi , you may be at risk of using rouge wifi setup by attackers by fake hotspots.

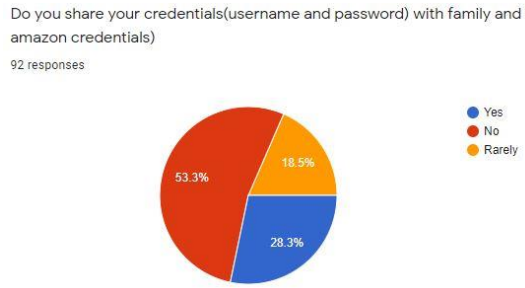


Password is used to get access of platform which is locked for security purpose. We use the password to secure Social Media, software, credit cards, mobile phones, laptops, desktop and many more from the unauthorized user. As password is used to secure but it is a weak form of protection for many reason. As the response from survey only 60.9% are rarely changing their password, the attackers try to guess the password constantly so if someone does not change the password regularly the chances of attack is more. If passwords are regularly changed the chance of attackers to attack time length will be reduced. From my survey response

of 92 only 1.1% is changing the password regularly, 32.6% monthly and 5.4% does not change their password.



Intention of this question was to know how many of them use the same password for more than one platform. From 92 responses 44.6% uses same password for more than one platform. If one of their platforms gets hacked the attackers can easily hack the other platform with same password. So it is important that no one should use the same password for more than one platform. 55.4% responded that they do not use same password for multiple platform.



From above graph 28.3% share their credentials, if the shared credential is used by the user for multiple platform and the shared credential is leaked from friends or family then the chances of vulnerability for other platform is more. 53.3% does not share their credential and 18.5% rarely share.

5. MOST COMMON CAUSES OF DATA BREACH

Every day we can see a headline regarding data breach occurred in a organization or government or individual in a newspaper or blogs. So to get away from such headlines the organizations or individuals should aware about most common causes of data breaches and what actions to be done. Latest news of data breach is big basket data breach over 2 crore data are leaked in darkweb.

- **Weak and Stolen credentials**

Every day users have to use multiple platform for multiple purpose it can be social media, software, system etc. And everything is protected by credentials, to remember different credentials its difficult. So the users use same credentials for multiple platforms or they note it down somewhere or keeping simple password to remember. All three method is wrong, if a hacker guess the password and he get it right then he can easily get into other platforms, if the book or laptop or smart phone stolen then the credentials are easily accessed by the attacker or if the password is weak then it is just a matter of time for hackers to guess.

- **Falling for social engineering tactics**

Without having knowledge or prior training it is difficult it understand the tricks from hackers. Opening links which contains malicious or giving sensitive data through calls or mails. Some of the attacks come under social engineering is phishing attack.

- **Connecting to public wifi**

Connecting to public wifi make the system vulnerable. Their network security will be compromised as they are open for public. Hackers can make malicious linked hotspot available in public places and the people connecting that wifi get vulnerable. Man in the middle attack is one of the common attack occur in open wifi

- **Outdated software**

Like food software also has short lifespan as technology grows. Outdated software's are not maintained due to which there will be patches which is vulnerable. So using the outdated software the chances of getting attacked is more. There will be some issues from development side to rectify that issue developer's launch the update and if the user doesn't update then the patch will remain same and hackers will take benefit of that patch.

- **Ignoring Security policy**

Developer's mindset is to make the software first to market due to which the security guidelines are totally ignored, in result make the software vulnerable for attacks. Some organizations have a policy where the employees have to change their password in regular interval of time, but it's difficult to change the password and remember each and every time. So the employees keep a simple and weak password which is easy to guess by the hacker.

6. WORST PASSWORD OF 2020

Here are the top 9 worst password of 2020 from Nordpass. The list contains number of users used the password, time to crack it and time exposed

Position	Password	Number of users	Time to crack it	Times exposed
1. ↑ (2)	123456	2,543,285	Less than a second	23,597,311
2. ↑ (3)	123456789	961,435	Less than a second	7,870,694
3. (new)	picture1	371,612	3 Hours	11,190
4. ↑ (5)	password	360,467	Less than a second	3,759,315
5. ↑ (6)	12345678	322,187	Less than a second	2,944,615
6. ↑ (17)	111111	230,507	Less than a second	3,124,368
7. ↑ (18)	123123	189,327	Less than a second	2,238,694
8. ↓ (1)	12345	188,268	Less than a second	2,389,787
9. ↑ (11)	1234567890	171,724	Less than a second	2,264,884

[4]Figure -1: Worst password of 2020 from nordpass.

6.1 New password Creation Guidelines

1. Using the lengthy password than complex password, decrypting lengthy password take more time.
2. Organizations have a policy to change the password in regular interval of times which make the employee difficult to remember the password and for ease create a weak password which is more dangerous.
3. Using alphanumeric and special characters.
4. Do not use any similar password to username.

7. HOW TO REDUCE HUMAN ERROR?

Using lengthy password, using automated safeguard such as cryptography, password management. Using Mutli-Factor Authentication. Organizing workshops on Social engineering, security management lectures. Audit on daily basis on security management. Updating the software as required to avoid vulnerable patches.

8. CONCLUSIONS

This paper shows how humans are paving way to cyber security. Many employees and individuals are falling into the trick of social engineering. How developers are ignoring security policy to launch the product first on market. How complex security policies are making the users to make mistakes. This is a big concern even if the organizations are investing in advanced security features but still breaches are occurring to human negligence. So on this topic it is clear that more research has to been done and have to make proper security guidance to reduce the human error.

REFERENCES

[1] What is Social Engineering? https://www.csoonline.com/article/2124681/what-is-social-engineering.html#:~:text=Social%20engineering%20definition-,Social%20engineering%20is%20the%20art%20of%20exploiting%20human%20psychology%2C%20rather,to%20buildings%2C%20systems%20or%20data..

[2] Data breaches by human error. https://www.venafi.com/blog/7-data-breaches-caused-human-error-did-encryption-play-role#:~:text=Human%20error%20has%20a%20well,87%25%20the%20previous%20two%20yearsR. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[3] Human error to blame most breaches.By Will R. Daugherty https://technews.tmcnet.com/cybersecuritytrend/topics/cyber-security/articles/421821-human-error-to-blame-most-breaches.htm

[4] Worst password of 2020 https://nordpass.com/most-common-passwords-list/