International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 11 | Nov -2016 www.irjet.net p-ISSN: 2395-0072

Analysis of the Human Factor behind Cyber Attacks

Anmol Singh[1], Bhaskar Kapoor[2]

[1]Senior, Department of IT, MAIT, GGSIP University, Delhi, India
[2]Assistant professor, Department of IT, MAIT, GGSIP University, Delhi, India

---

Abstract - *The following paper is associated with the human factor behind the data breaches in the cyber world. We start by presenting examples of some data breaches from the recent past caused due to the, deliberate or inadvertent, human errors. We then look at some statistics drawn from global cyber trends of data breach events. The causes of data breach and cyber-attacks are presented. A very important factor jeopardizing the data security, social engineering, is then examined. Factors influencing the humans in the social engineering techniques are also explained.*

Key Words: Cyber-attack, Data breach, Human factor

1. Introduction:

A Cyber-attack is a malicious attack on a computer system for information, access of a network or the components linked with that network. The attack may be led by an individual or an organization as a whole. The aim of the attack can be to steal or alter the information in a computer or to destroy the network/computer system.

In today's world, cyber-attacks are one of the greatest concerns of the digital world. With the increasing number of organizations moving to cloud, the risk of data theft is at an all-time-high. The sensitive and confidential nature of the information calls for methods of computer security. The large number of cyber-attacks at some of the biggest organizations and governments in the world has proved that more attention is required in the field of data security. These attack events have proved that no matter how secure systems are in place, the information on the web is always at a risk of being stolen. All this calls for a major transformation in the implementation of ways that the security systems are installed.

The three basic elements crucial for a successful organizational transformation are- People, Process and Technology. For a long time, the efforts made for an organizational and infrastructural transformation have concentrated on the process improvement strategies and business process re-engineering, i.e. focusing major use of resources on process and technology, while essentially ignoring the factors related to the people in the initiative. And so, it does not come as a surprise that these transformation initiatives have not been able to achieve their desired goals. A recent study has shown that 75% of the organizational transformation initiatives have either completely failed or haven't been able to achieve their desired objectives in the long-term.

For a holistic solution to exist, the People should also be considered as a part of the transformational focus. In most of these suggested solutions, it has been seen that the technology and processes implemented can be made "State-of-the-art" by spending hard dollars, but improvement in the part of the people takes more than just money. What seems to be the crucial issue is that the people (or the users) tend to rely too much on the technology to protect them, while they also play a very vital part in the process of data security.

It has seemingly become a popular perception that technology is the only factor that can guarantee safety and security for people in the online world. Let us make it clear, technology is not a Panacea. Even after huge investments in order to improve technological infrastructure, the cyber-attacks keep happening. One of the reasons for this is that, nothing, even in this age of technology, can replace the role of people.

2. Recent data breaches caused by human error [1][3]:

2.1 Ebay: In 2014, a group of attackers stole login credentials of as many as 100 ebay employees through phishing attempts.. The information was used to get into the internal network, where they downloaded names, physical addresses, email addresses, passwords and other personal information of 145 million customers.

2.2 Anthem: In 2015, the health insurance company revealed that attackers were able to get their hands on both consumers' and employees' personal information. The attackers stole the admin's login credentials using social engineering techniques. In this breach, more than 80 million customers were affected, which cost around $31 billion USD to the company.

2.3 JPMorgan Chase: In spring 2014, the login credentials of one of the employees of the company were stolen by the hackers, who then exploited an oversight- there was no 2-step verification in the bank's security system for one of the servers, to hack into the company's corporate network. Following the initial attack, the hackers were able to gain access to a total of 90 servers.

2.4 Target: In November 2015, the attackers were able to install malware on the POS terminal at one of Target's store, by using network credentials stolen from Fazio Mechanical services. The attackers gained access to about 40 million credit and debit card records, as well as about 70 million personal information records, which cost Target around $105 million.

2.5 Home Depot: In September 2014, attackers were able to get into the retailer's network using login credentials of a third party vendor and installed malware onto 7500 self-checkout systems in the US and Canada. Details about 56 million customers' credit and debit cards as well as 53 million customers' email addresses were stolen.

2.5 NHS Trust: In September 2014, a staff member of the 56 Dean street clinic accidentally sent out a newsletter that allowed all recipients to view every other subscriber's email address and full names of 730 of those 781 subscribers. . In response, a fine of £180,000 was issued against the trust.

2.6 Pentagon: In July 2015, a spear-phishing attack was used by the attackers to hack into the Pentagon's email system and leak the stolen information online. The attack affected about 4000 military and civilian personnel.

2.7 Sony Pictures Entertainment: In 2014, the attackers stole the login credentials of Apple accounts of many of Sony's top executives through a phishing attack. The attackers stole about 100 TBs of data from the company's computer networks.

2.8 Ubiquiti fraud: The attack against Ubiquiti finance department resulted in a transfer of funds of about $46.7 million from the company's Hong Kong subsidiary to other third party overseas accounts. It was determined later an outside entity made "fraudulent requests" and involved "employee impersonation."

2.9 Facebook: In 2008, the dates of births of about 80 million users were accidently made publicly accessible while upgrading to a new website design.

3. The Human Factor in Cyber Crime and Cyber Security:

One of the most intriguing findings from IBM's 2014 Cyber Security Intelligence Index [4] is that "95 percent of all security incidents involved human error".

According to Verizon's Data Breach Investigations Report 2013 [5], up to 95 percent of advanced attacks involved spear phishing tactics with emails containing malicious attachments that could potentially download malware onto the user's computing device". This gives attackers an entry-point into the organization from which they can move laterally in search of valuable information, such as intellectual property.

The IT Policy Compliance Group says that 75% of ALL data is lost due to human error. The Aberdeen Group marks this figure at 64%, CompTIA says that 52% of security breaches were a result of human error and most recently, Databarracks said employee accident was the top cause of data loss (24%).

According to a recent study in UK by the Security vendor Eset, as many as 22,000 USB sticks were left with the dirty clothes and handed over to the UK dry cleaners every year, with nearly half of those never returned." Not just this, around 973 mobile phones were left inattentively with the laundry and handed over to the cleaners, the study found.

According to the PWC Information Security breaches Survey 2015 [6], 50% of the worst breaches in the year were caused by inadvertent human error, up from 31% a year ago. 75% of large organizations and 31% of small organizations suffered staff-related security breaches in the last year as compared to 58% and 22% respectively, a year ago. 72% of companies where the security policy was not clearly understood had staff related data breaches. 28% of the worst security breaches were caused to some extent by senior management not giving sufficient priority on security.

4. Root causes of data breaches:

A recent study by the Ponemon institute [7] identifies the following activities as the most common risky causes of data and network breaches:

1. Using an insecure network for connecting computers to the internet.
2. Not deleting information that is no longer necessary from the computers.
3. Sharing passwords with other employees.
4. Reusing the same login credentials on different websites.
5. Using Unencrypted USB drives.
6. Leaving computers unlocked when not around.
7. Losing a USB drive with confidential data and not reporting it to the organization immediately.
8. Working on a laptop while traveling and not using a privacy screen.
9. Carrying confidential information on a laptop unnecessarily while travelling.
10. Connecting personal mobile phone to the organization's network.

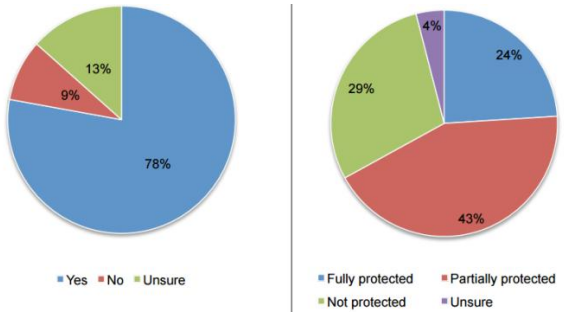

Figure 1: (Left) Has your organization ever experienced a data breach as a result of negligent or malicious employees or other insiders?
Figure 2: (Right) In general, is your organization's sensitive or confidential business information protected by encrypted or other data protection technologies?

The Ponemon report [7] clearly states that Employee negligence or maliciousness is the root cause of many data breaches. According to Figure 1, over 78 percent of respondents reported that negligent or malicious employees

or other insiders within their organizations were responsible for at least one data breach over the past two years. Figure 2 shows that 43 percent and 24 percent respondents report that their organization's sensitive or confidential business information is protected partially and fully respectively by data protection technologies such as encryption and data loss prevention (DLP).

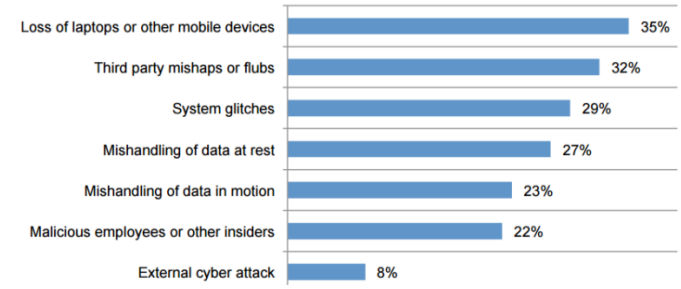

Figure 3: What were the root causes of data breach incidents experienced by your organization over the past 12 to 24 months?

Employees' loss of a laptop or other mobile devices, third party mishaps or flubs and system glitches are the top three root causes of these breaches.

Employees' lack of attention towards data protection and an increase in sensitive data on mobile devices is putting sensitive and confidential information at risk. Figure 4 shows employees frequently (37 percent) or very frequently (19 percent) store sensitive data on their laptops, smartphones, tablets and other mobile devices.

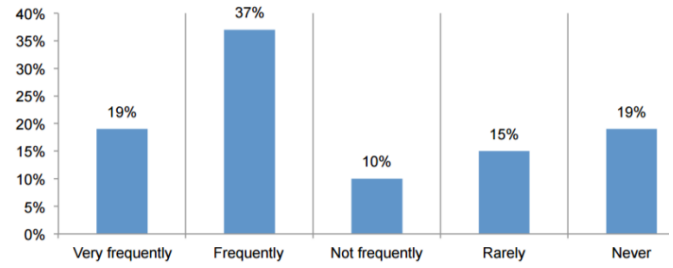

Figure 4: How frequently do employees carry sensitive data on their laptops, smartphones, tablets or other mobile devices?

5. Differences between smaller and larger-sized businesses:

The Ponemon institute report [7] states that human factor risks are more frequent in small-sized companies (SMBs) than bigger enterprises. Figure 5 shows the 10 human factor risk categories with the widest gaps between small and large organizations. In every case, we see that the SMB subsample reports a higher percentage response as compared to the enterprise subsample. Specifically, we see that the largest difference (19 percent) appears on the "employees open attachments or web-links in spam." The second largest gap (15 percent) is associated with "employees leaving computer unattended," and a 14 percent gap for "employees do not change passwords periodically." There is a gap of 12 percent for "employees who visit websites that are considered off limits."

Smaller organizations have a bit higher rate of data breaches due to negligent or malicious employees or other insiders.

According to respondents in smaller organizations, the main causes of breaches are system glitches and employees' mishandling of data in motion. This is opposed to the respondents in larger organizations who report that it is the loss of a laptop or other mobile data-bearing device followed by third party mishaps or flubs.

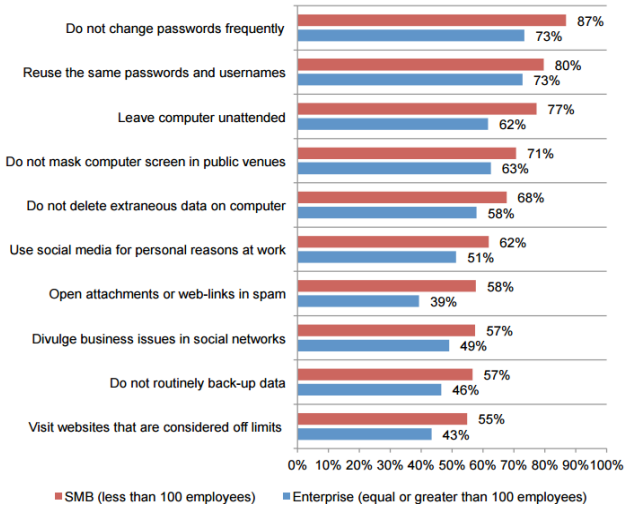

Figure 5: Human factor difference between SMB and Enterprise organization.

6. Worst Passwords of 2015:

SplashData's fifth annual "Worst Passwords list" shows how people have continued to putting themselves at risk. "12345678" and "password" remain the worst passwords, holding the top positions in the SplashData's first list since 2011.

The list compares data for 2 million leaked passwords. The report shows that though people have started using longer passwords such as "1234567890" and "qwertyuiop", the extended length plays no significant role as the longer passwords are still very simple.

New passwords that appeared on the 2015 list that did not on the 2014 list are "Welcome", "login" and "passw0rd". In recent years, simple numerical passwords have stayed the most common, being 6 of the top 10 worst passwords.

A popular password theme is that of sports and movies. With "baseball" already a popular worst password, a new password "football" has joined the league. Passwords like "starwars", "solo" and "princess" are new additions to the list.

The CEO of SplashData, Morgan Slain says, "We have seen an effort by many people to be more secure by adding

characters to passwords, but if these longer passwords are based on simple patterns they will put you in just as much risk of having your identity stolen by hackers. As we see on the list, using common sports and pop culture terms is also a bad idea. We hope that with more publicity about how risky it is to use weak passwords, more people will take steps to strengthen their passwords and, most importantly, use different passwords for different websites."

Rank	Password	Change from 2014
1	123456	unchanged
2	password	Unchanged
3	12345678	Up 1
4	qwerty	Up 1
5	12345	Down 2
6	123456789	Unchanged
7	football	Up 3
8	1234	Down 1
9	1234567	Up 2
10	baseball	Down 2
11	welcome	New
12	1234567890	New
13	abc123	Up 1
14	111111	Up 1
15	1qaz2wsx	New
16	dragon	Down7
17	master	Up 2
18	monkey	Down 6
19	letmein	Down 6
20	login	New
21	princess	New
22	qwertyuiop	New
23	solo	New
24	passw0rd	New
25	starwars	New

Figure 6: SplashData's fifth annual "Worst Passwords List" 2015

6.1 SplashData offers 3 simple tips [7]:

1. Using passwords or paraphrases of twelve characters or more with mixed characters.
2. Avoiding the use of same passwords over and over again on different websites.
3. Using a password manager such as TeamsID for organizing and protecting passwords, generating random passwords and automatically logging into websites

7. Common mistakes employees make:

In an article published in June 2015, Trend Micro presents some common mistakes employees make:

- **Lax email habits** – careless opening of suspicious emails containing malware frequently leads to the download of malicious files, or landing on websites that cybercriminals use for phishing information that they can use.
- **Weak passwords** –short, weak and sometimes exposed passwords are commonly exploited by hackers and are one of the easiest ways to hack into a system. In addition, some employees often share their passwords with others.
- **Falling for social engineering tactics** – without prior knowledge or training about such techniques, it could be difficult to avoid social engineering traps like social media scams, malware and spam that ride on the popularity of big news and events, or others.
- **Poor backup practices** – employees often fail to back up data which increases the downtime and losses incurred when an organization is attacked.
- **Poor security habits outside work** – employee devices are inherently insecure, unlike the company-owned devices. They often have potential vulnerabilities—either on the device or the operating system level that can be exploited.
- **Connecting to unsecured Wi-Fi networks** – employees connect to open or public Wi-Fi networks that can allow attackers to capture traffic from an open access point and launch attacks such as man-in-the-middle (MITM) attacks.

7.1 How credit cards allow attackers to cash in:

The IBM Security Services 2014 Research report explains this. The average credit card sells for anywhere from $25 to $100 in the black market, depending on the available information in the card data—such as CSV security code, expiration date and known limits. Once the stolen cards are acquired by he attackers, they are moved into elaborate laundering schemes where they are used to buy gift cards and prepaid credit cards. The shuffling of funds is continued as these "untraceable" cards are used to purchase other items that can then be sold online with no links to the original card data.

8. Social Engineering:

The University of Pennsylvania's Desktop Security 101: A Quick Course in Safer Computing gives a witty definition of social engineers:

"Social engineering" is a term that has come into use in the computer security field over the last few years to describe the activities of what are, essentially, con men (and women). Their game is to get someone to willingly give them privileged information by exploiting some combination of:

- The innate, good-natured desire to be of help to a fellow human being.
- The belief that everyone basically honest.
- The person's current state of being extremely busy and distracted.

- The belief that bad things happen only to other people.
- Stupidity.
- All of the above

A cyber awareness report by Axelos [11] explains social engineering as the work of a con artist, trickster or fraudster who is trying to play on willingness of people to help and to manipulate them to share confidential information. Social engineers may email or phone people, pretending to be someone they are not. This could be someone from within the organization, e.g. the Help Desk, or from a trusted organization, e.g. your bank.

The objective is still the same – to access information. This can be a username, a password, bank details, personal details, etc. Social engineers are usually trying to get access to your network or personal computer/device so they can install malicious software which will allow them to steal sensitive information.

Figure 7: The Following Infographic by the Symantec Corporation [10] explains how the Gmail Scam works.

Schneier (2000) explains that there are 5 steps that ensure the success of a social engineering attack. First, the target is chosen and all information relevant concerning that target is collected. Such information includes job advertisements, company brochures, published reports tender documents and any other information publicly available, with the aim of gathering enough to heighten the legitimacy of the attack (Aiello, 2008). Second, the collected information is then analyzed and a vulnerability is determined, which can be used to reach an objective. Third, access to the target individual is established. After all this preliminary work is completed, the attack can be performed. Finally, the attack is completed and all evidence related to the attack is destroyed or removed (Schneier, 2000).

8.1 What makes People Susceptible?

There are a wide number of factors that often tend to increase an individual's susceptibility to social engineering attacks. Generally, attempts for social engineering are more likely to appear legitimate if the attacker is able to form a relationship of trust with the victim, making them more vulnerable to intrusion.(Aiello, 2008).

8.2 Psychological Triggers and Individual Factors that Increase Susceptibility:

According to Workman (2008), susceptibility is greatly connected with individuals' likeability and trust, and people who are more trusting are more likely to capitulate to social engineering attacks. Mitnick and Simon (2002) explain that it is human nature to trust people, particularly when their requests seem equitable, and when they do not have any reason to be skeptical. Generally, people have a desire to be helpful, but they often lack appropriate assertiveness. Hence, social engineers use this knowledge to exploit people, and often attempt to build a friendly accord with them, knowing that victims are more likely to fulfill all requests if they like or trust the attacker (Gragg, 2002).

Another effective technique involves creating a heightened emotional state with the victim, which enables the attacker to make requests that might otherwise be refused under normal circumstances (Gragg, 2002). When emotions like excitement, anger, surprise, panic or fear are heightened, the victim becomes more likely to be easily distracted, and less likely to logically evaluate and enquire the attacker's story (Gragg, 2002). Similarly, feelings of guilt or moral outrage can also reduce an individual's ability effectively to logically validate any requests. Social engineers may therefore create situations designed to produce empathy, and the victim may agree with the request in order to help diminish the requester's problem (Aiello, 2008).

Essentially, when people have a feeling of attachment or emotional bond to the social engineer, they are more likely to feel committed to disclose sensitive information (Workman, 2008). Generally, peoples' level of commitment affects their susceptibility, and people who have higher levels of commitment are more likely to fall prey to social engineering attacks. This is also supported by Cialdini (2006), who argues that once someone has made a decision, they then feel pressure to remain consistent with that decision, and this pressure is often strong enough for people to act in ways that are different from their own interests. This idea is referred to by Workman (2008) as Affective commitment.

Related to this, Workman (2007) also describes Normative commitment, which is associated with the idea of returning the favor. Evidence suggests that people like to reciprocate when they have been helped or have received a benefit (Cialdini, 2006), and people who are more normatively committed than a random person are more

likely to feel obligated, and hence, are more likely to capitulate to social engineering.

Reverse social engineering tactics involves a situation where the attacker creates a problem, and then offers to assist the victim (Aiello, 2008). Since the victim is not aware that the attacker was the one to create the problem, he or she is likely to want to show thankfulness or appreciation by helping the attacker with any subsequent requests.

Requests are also more likely to be accepted if the victim is overloaded with information. Hence, when flawed arguments are heard promptly, and are listed together with convincing truths, people are more likely to be burdened, and are therefore less likely to question the accuracy of the facts (Gragg, 2002). Similarly, people are also less likely to enquire about unreasonable requests when they are faced with time pressure. Therefore social engineers choose to often call at unexpected or inconvenient times (such as at the end of the day) and will often indicate that a particular item or offer is meagre or only available for a short period of time (Cialdini, 2006). Evidence suggests that people tend to desire something more when there are limits placed on their ability to obtain it (Cialdini, 2006).

Evidence also suggests that social engineering is more effective when a factor known as diffusion of responsibility is employed (Gragg, 2002; Aiello, 2008). Essentially, individuals are more likely to make decisions or provide information if they don't feel solely responsible for any consequences. Hence, the social engineer will often create situations designed to diminish the individual's feeling of personal responsibility, and the victim may then be more willing to help the attacker (Gragg, 2002). This could include the claims about the individual's colleagues already providing similar information, as the individual may then want to conform.

8.3 People-Related Issues in Computer and Internet Security:

Asgarkhani and Sitnikova from University of South Australia created a list of issues related to people that directly impact their organizations' safety:

- A relaxed culture where reliability of the system is not taken seriously.
- Lack of understanding and awareness of implications of compromises in security.
- Lack of training to admin staff so they can understand the functions and risk implications.
- Lack of training about management to be aware of value of security and cost of being exposed to risks to their businesses.
- Shortage of suitably trained, skilled and technical staff to manage the operations of the system.
- An environment where there is less emphasis on teamwork.
- Cultural differences in multicultural environments where crashes among cultures may also result in teams unable to work together towards shared outcomes.

9. Results:

This paper clearly documents the data which proves that human factor is the major contributor to the data loss and data breach events. Many employees in the IT sector fall prey to the social engineering tactics of the attackers and end up compromising the confidentiality of the organization's data. The paper shows that negligence or misdemeanor on part of the employees often leads to data breaches. This cannot be allowed to continue due to the sensitive nature of the data. Now the challenge is to devise new techniques that equip the employees against such wrong tactics. So there is clearly a need for further research in this area for improving cyber security.

10. References:

1. People's Role in Cyber Security: White Paper by Crucial Research, Available at: https://www.crucial.com.au/pdf/Peoples_Role_in_Cyber_Security.pdf
2. 8 Data Breaches Caused by Human Error, MetaCompliance Blog, Available at: http://www.metacompliance.com/blog/8-data-breaches-caused-by-human-error/
3. The IT Governance Blog at "Five damaging data breaches caused by human error", Available at: http://www.itgovernance.co.uk/blog/five-damaging-data-breaches-caused-by-human-error
4. IBM Security Services 2014 Cyber Security Intelligence Index research report. Available at: https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf
5. Verizon's 2013 Data breach Investigations repor, Available at: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf
6. Information Security breaches Survey 2015, conducted by PWC, Available at: http://www.pwc.co.uk/assets/pdf/2015-isbs-executive-summary-02.pdf
7. Ponemon Institute Research Report on "The Human Factor in Data Protection", Available at: http://www.ponemon.org/local/upload/file/The_Human_Factor_in_data_Protection_WP_FINAL.pdf
8. SplashData's fifth annual "Worst Passwords List" 2015. Available at: http://splashdata.com/blog/
9. Data Breaches and the Human Factor, Available at: http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/data-breaches-and-the-human-factor-are-employees-the-best-defense-or-the-weakest-links.
10. Symantec press release, Available at: http://www.symantec.com/en/uk/about/news/release/article.jsp?prid=20130605_01
11. Axelos's report on cyber awareness , Available at: https://www.axelos.com/Corporate/media/Files/cyber-awareness.pdf
12. Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering

threats to information security. Journal of the American Society for Information Science and Technology, 59(4), 662-674.
13. Aiello, M. (2008). Social engineering. In L.J. Janczewski & A.M. Colarik (Eds.), Cyber Warfare and Cyber Terrorism (pp. 191-198). Hersey, PA: IGI Global.
14. Cialdini, R.B. (2006). Influence: The Psychology of Persuasion (Rev. ed.). New York: HarperCollins.
15. Gragg, D. (2002). A multi-level defense against social engineering. White paper, SANS Institute, Retrieved on June 12, 2008 from http://www.sans.org/rr/papers/51/920.pdf
16. Schneier, B. (2000). Secrets and Lies: Digital Security in a Networked World, Indianapolis, IN:
Wiley Publishing, Inc.
17. Australian Government department of Defense's report on "Human Factors and Information Security", Available at: http://www.dtic.mil/dtic/tr/fulltext/u2/a535944.pdf