Hacking the Human

CIS4012-N-BF1-2018

Word Count: 5115

Thomas Ruddock

Q5114161

Julie Turnell

Teesside University

Contents

Introduction 2
1. Part 1 2
1.1. Introduction 2
1.2. Analyse case study using (framework) 2
1.3. What is the attack vector? (how it happened) 3
1.4. What channel(s) was used? 4
1.5. Who is the operator or actor who originated the attack? 4
1.6. What approach did they use? 4
1.7. What human weakness or attribute were they targeting? 5
1.8. Discussion and evaluation 6
1.8.1. How easy was the approach to apply? 6
1.8.2. Did all the important elements of the attack been identified? 6
1.8.3. Would the same approach be used on this type of attack again? 6
2. Part 2 6
2.1. Introduction 6
2.2. Appropriate solutions that would help mitigate against similar issues occurring again 6
2.2.1 Training 6
2.2.2 Behavioural & Procedural 7
2.2.3 Policies 8
3. Part 3 9
3.1. Introduction 9
3.2. Ethical Issues 9
3.3. Moral Issues 10
4. Conclusion 10
5. References 11

Introduction

This report will be analysing a real-world case study which includes a cybersecurity breach, which was originated through the social engineering attack vector or vectors. This report will have four main sections and a reference section at the end of the report. Section one also called part 1 will be the analysis of the cybersecurity breach using a framework which is the Ontological Model which will help the analysis of the attack vector. Section 2 also called part 2 will be talking about the proposed interventions that can be used to mitigate against these types of attacks. Section 3 also called part 3 will discuss the ethical and moral issues of the human behaviour within an organisation. Section 4 will round the report altogether in a conclusion. Then section 5 will be the references which will be displayed in a Harvard reference style and in alphabetical order for the reader. Each main part of the report (part 1, part 2, and part 3) will have an introduction to talk about the sub-sections of the section.

1. Part 1

1.1. Introduction

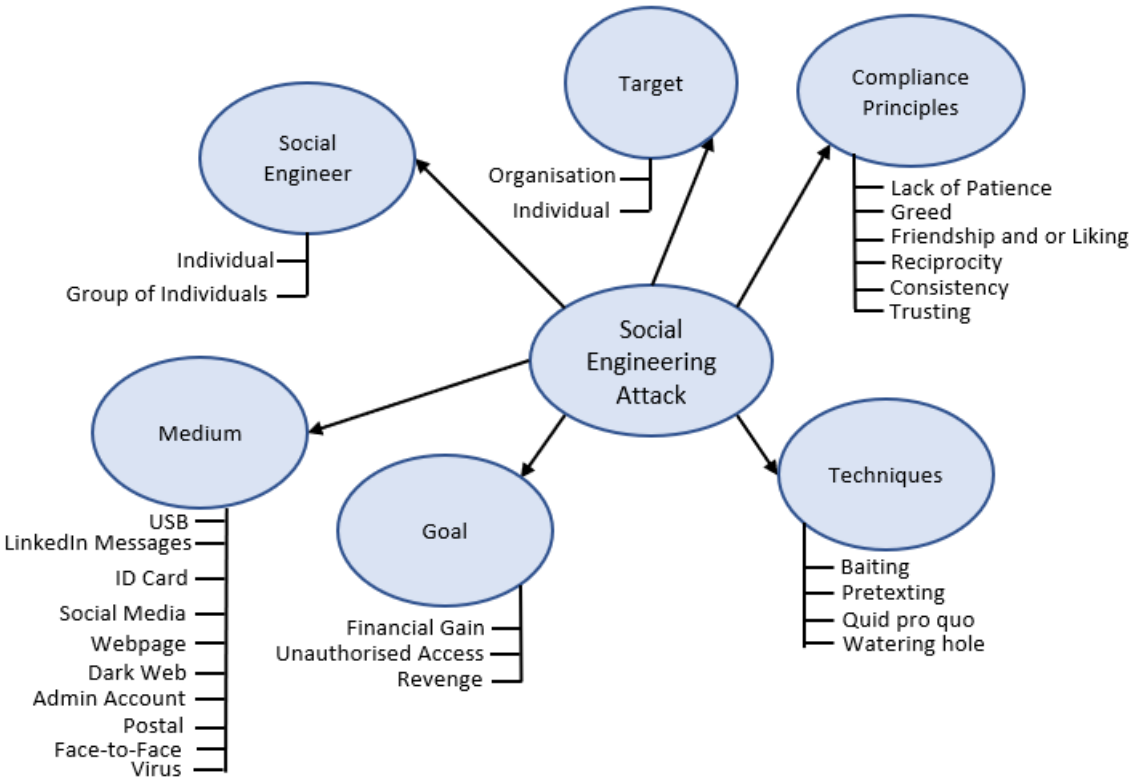
Part 1 of this report will have multiple sub-sections, which include the framework which will be used to analyse the breach, it will additionally include the attack vector which shows the method how the hacker accomplished the breach, and the next one will be the channel that was used to create the breach. After that will be to identify the operator(s) and or actor(s) who originated the attack. The next sub-section will show the approach they used to perform the attack. After that is what human weakness or attribute were they targeting to make the attack successful. Then finally is the Discussion and evaluation which has its own sub-sections which includes how easy was the approach to apply, did all the important elements of the attack been identified and would the same approach or framework be used on this type of attack again?

1.2. Analyse case study using (framework)

The framework which was decided to be used to analyse the cybersecurity breach is the Ontological Model, which will be used to analyse the social engineering attack. In these sub-sections of part 1, we will be analysing the engineering attack with the diagram to show the process of classifying information, which will create a taxonomy of classes and will display the relationships between them, Van Rees (2008) provided information for the visit.

The Ontological Model of the social engineering attack will have a main class with six subclasses called ‘target’ which show who the social engineers target is from this attack, next is the who is the ‘social engineer meaning if it is a lone wolf or multiple people, after that is the ‘medium’ which lists all of the ways the SE gathered the information or used before, during and after the attack. The next class is ‘goal’ which will show the goal of the social engineer, for example, financial gain, revenge, etc. After that is the ‘techniques’ which were used to get information, for example baiting, pretexting, etc. Then finally is the ‘compliance principles’ which were used to gain access to the data, for example, friendship or liking, Authority, social validation, etc. Tiwari (2018) provide information for the visit.

All of these will maintain the classes and activities that were used for this social engineering attack and will help to analysis the attack and undertake proper action to fix these holes for the future.



The diagram above will display the classes used to identify and help analyses the three social engineering attacks or incidents. The first attack includes a previous employee Jamie Smith who helped the attacker calling himself Sam. The second attack was from some employees which searched and navigate an infected website about a Fantasy Football League which caused the network to be infected with a ransomware virus. And the last incident is when Janice plugged an unknown USB into her work computer, which she thought it was the fault for the ransomware attack.

1.3. What is the attack vector? (How it happened)

There are three social engineering attacks going on around a similar time. The first one was when Jamie Smith could resign and work a week's notice, to give him respect since Jamie's dad worked with Brian in the early days of the company. During Jamie's last week of work, he becomes angry and posted several posts on Facebook and LinkedIn. At the end of the week, he received a sympathetic LinkedIn message from someone calling themselves Sam. He responded to the messages saying he will have money problems while seeking a new job. Sam subsequently gave Jamie an olive breach by offering money (5K) and send his ID card for the company. Sam said they are a competitor and want to perform some reconnaissance then send the ID card back to Jamie. Jamie accepted the offer. After a couple of days, Janice encountered an unknown person wandering around the offices and hovering around the desk of colleagues who were on holiday. She then challenged the person, and they left in a hurry, she then called the police and checked the CCTV which showed the mysterious man was there all morning, people have spoken to him and give them a plausible statement, so people don't expect anything. Rob then checked the computer logs which turned out to have a new admin account which was created that morning showing the person was doing something malicious, the account was them shut down. The company then called a cybersecurity specialist to examine the system and discovered that the employee's payroll records have been copied and sold on the dark web.

The second attack starts with Janice discovering a strange USB on the floor, and she took the USB and wanted to find out who it belongs to. After doing morning business she then turns to the USB and plugs it into her PC which happened to be an admin account and uncovered no information to identify who it belonged to. Five Minutes later a ransomware pop-up appeared on all PCs in the admin offices. Janice genuinely thought it was her fault and when to Rob to convey what has happened. Rob started the backup process and coupled with a decryptor tool. Which reverse the network back one day and lost a full business workday, they restored, re-installed to the latest back-up. The third attack was after the investing took place and shows Janice was not at fault and it turns out it was one of the workers on the shop floor accessed a dodgy website about Fantasy Football League which was infected with the ransomware virus. It was said it was difficult to ascertain if the company had been targeted or it was an opportunistic attack.

1.4. What channel(s) was used?

The channels used for these attacks can be found on the Ontological Model under the medium class, which shows what has helped archive these breaches.

The first breach with involves Jamie and Sam, the medium used, was the LinkedIn messaging function of social media to make contact with Jamie, then Postal services were used to move the ID card to and back from Jamie and Sam, the ID Card to gain access to the building and not to invite suspicion, then face-to-face to minimise suspicion again, then the Admin account to be able to steal the payroll records, finally the Dark Web on where the sensitive data was sold on most likely used bitcoin to be untraceable.

The second breach involves Janice, the medium used, was the USB. Which looked like was the trigger for the ransomware attack.

The third breach involves hackers and the floor workers, which would have used web pages and virus for the medium. Which the worker accessed the website and the virus attacked the companies' computers.

1.5. Who is the operator or actor who originated the attack?

In the first attack there are two operators and or actors, the first one is Jamie, because he was posting angry post on social media, which drawn the second actor in to offer Jamie money for his ID Card to get into the building, The operator then used the ID Card to gain access to the building and we believe he creates an admin account and copied and sold the payroll records on the dark web. But Jamie didn't think it was going to be malicious by the LinkedIn messages.

The second incident or attack is when Janice plugged an unknown USB what could have been malicious towards the organisations, which Janice through that happened when the ransomware pop-up occurred. Therefore, Janice would have been the operator and or actor if it was a malicious attack.

Then the third attack was originated by a worker employee accessing websites they shouldn't have during work hours, but because of the lack of policies about that it put the companies' security at risk and lost a full business work day. You could also argue that the companies firewall was not strong enough to prevent this from happening.

1.6. What approach did they use?

The first attacker approach was using the anger and wanting to have revenge on the company from Jamie to gain access through an ID card which got the unknown person passed security. In addition, the person created an admin account from other colleague's computers since they were on holiday,

he could have gained access through Jamie's account that might not have been deactivated yet or could have found the password for the computer on or around the workstation. Once logged, he could copy and download the payroll records on to a USB or external HDD for security and will leave no trail. Once he got confronted by Janice, he fled the site and later that day he could have sold the sensitive information on the Dark Web and Jamie will get his money and ID card back a few days later.

The second incident looked like someone lost and or placed a USB on the floor for an employee to access and risk a network attack, but luckily it was Mike's son's homework. If it was malicious, it would look like they aimed for the company because of its lack of policy in that area.

The third attack is a little different because an infected website was created to catch or entrap players of the Fantasy Football League looking to obtain enhancements at an offer. Once the hackers have created the site, they will make it look credible and infect it with the ransomware virus by using a watering hole method. Once this is done, they just need to wait for a victim to trigger the malicious code and have the computer looked and won't open unless the user pays the fee and that's what happened to some workers where browsing the internet and come across a new site for this game and was tricked to open the site and all the computers had a pop up for ransomware.

1.7. What human weakness or attribute were they targeting?

Everyone has human weakness or bad attributes to computing activities if the employee has not received proper training courses about these issues. Hence, it would be effortless for an SE to target these kinds of people with no awareness, in most companies only the admin teams know about kinds of threats. The first attacker was exploiting Jamie's weakness at the time was anger and revenge, they also used trusting attributes for Jamie which he was waiting for 5K and the other employees to talk to Sam when he was on site he additionally would have used reciprocity which treats others how they treat you, he also could have used scarcity making it look like he is doing something, he would not be talked to as much.

The second attack and or incidents would have used the lack of knowledge of these issues to do with the policy of plugging unknown devices into workstations on a network. The weakness of curiosity to examine what the USB holds might be too much for some people by not having self-control.

The third attack will have similar weakness and attributes to use or exploit. The first and main one for the hacker is to make the website look professional and trusting making the victim feel safe before infecting the PC or network system, The next one will be the patience part for the hacker because once they have finished the site they just have to wait for a user to bite and access the site and hope they acquire money from the user if they are not tech smart on how to avoid the fee and eliminating the virus. The following bit is what the hacker wants the user to have weakness or bad attributes to be tricked. The victim possesses the type of weakness that the hackers are aiming for the trusting of legitimate looking sites and lack of patience if the user waited until they concluded work and carry out this activity at home the full network would not have to been attacked and rerolled back one-day losing money for the company. Greed will also pop its head into the equation as most if not all people want a deal and if it looks good some people might go for it.

Scam statistics say in 2018 ransomware & malware scams have been reported up to 4 356 times with 2% with financial losses which add up to $151,195, Scamwatch (2018) provided information for the visit.

1.8. Discussion and evaluation

This sub-section is a small and brief about the discussion and evaluation of the analysis section. It includes how easy was the approach to apply, did all the important elements of the attack been identified and would the same approach be used on this type of attack again.

1.8.1. How easy was the approach to apply?

It was not easy but not challenging at the same time, as reading through the scenario it is semi-easy to find where the critical information goes to find out what is merely behind the attack. Very easy to understand the framework so not much can go wrong.

1.8.2. Did all the important elements of the attack been identified?

Yes, the important elements have been identified, maybe some small data points might have been missed out, but the most valuable stuff is there.

1.8.3. Would the same approach be used on this type of attack again?

Yes, the Ontological Model or framework used was extremely good for this type of attack but maybe it should be modified if more than one attack has taken part, so maybe three models one for each attack will make it easier to understand which elements belong merely to which one. So, if only one attack or breach has occurred it would work better with this Ontological Model than with three attacks.

2. Part 2

2.1. Introduction

This section is Part 2 and will talk about the appropriate solutions that will help mitigate against similar issues from happening again, the solutions will align with the findings from the analysis and will be supported by research and readings.

2.2. Appropriate solutions that would help mitigate against similar issues occurring again

In this sub-section will include three sections which will talk about the training and courses and why it is significant to obtain these when working in an organisation. After that is the behavioural and procedural section which will mention the way the company culture will tolerate certain behaviour and how they would like them to act and procedural will encourage the employees to have a more appropriate behaviour if it is backed up by the management and have rules and regulations if they are broken. Then the final one will talk about the policies which need to be implemented to prevent these attacks from happening again.

2.2.1 Training

Training can be incredibly difficult and easy to understand at the same time since they are countless training courses and in-house training courses that might suit the company more. Many training courses cost a lot of money if the full company needs to have security awareness training for all employees. These courses are about teaching and to understand the risks and threats around every corner, Saceanu (2016) provided information for the visit. Security awareness training can be very basic for only £100 for course which can be completed online, up to the ISO 27001 course which cost differently depending on how many people are wanting the certification for example 1 to 45 people will cost around £2,850 to £5,700. Itgovernance (2018) provided data for the visit. Just from the pricing of the training course, it will show you that it has different levels of superiority to them since

Watson's Widgets have 250 staff with three in the management and 50 in the payroll, admin and accounts job roles. The best thing for them is to have them trained at a higher level than the rest of the staff. For example, ISO 27001 and 27002, this is to save money for the company and have the rest of the staff take a basic training course or have the new ISO trained staff makes an in-house training program with the section of knowledge which goes around their job role.

Most if not all people have gone through training awareness even if it is from secondary school, college, university or their place of work, which would be the health and safety presentations, and we all know how boarding it can be even if it only half an hour long, most people will not listen or forget about it. So, to make the knowledge sink in the company can use humorous videos to keep people attenuation and have a written quiz at the end of the training course or presentations, which will make the staff pay more attenuation to it and if they fail they will have to undergo the course again. All these can be used in the policies or procedural section of the company. Based on past research if the company suggest several steps that should be taken before, during and after the training course it can maximise the impact of a program to the staff. Salas (2012) provided information for the visit.

Most basic security awareness training entails the password best practices, email, and browser security, social engineering which would have helped in these current attacks to the company, avoiding malicious downloads, mobile security, social media security, anti-virus, and software updates, secure remote working, physical security and protecting cardholder data. If the staff was trained in these areas before the breach, it wouldn't have happened, but training alone cannot help the staff they will need to incorporate the training, behavioural, procedural and following the recent policies which will be talked about in the next couple of sections.

Since everyone is different there is a different type of approach depending on the practical applications of the genal learning theory and on other theories and models to the industrial psychology. So, because of training research can be attributed in part of the evidence-based prescriptions for the design and delivery of training to staff. The science has been keeping up with the demand for training, they have found and analysed many empirical studies that go across various training topics from the team-training to management training. Salas (2012) provided information for the visit.

Because training is critically important to the workforce it can provide a competitive advantage to the company it does make sense to implement the best training program the company can afford for the correct people. Salas (2012) provided information for the visit.

2.2.2 Behavioural & Procedural

Behavioural skills are very important for modern companies more than ever. Behavioural skills are very different to training in a workplace because training is learned from the environment you are in and will change depending on the job role or what occupation you are in. But most behavioural skills are learned from a youthful age and are social in nature. By having these are learning these skills from a company culture it will make and draw out the productivity of the staff.

The 5 most essential skills which staff must develop or improve on is the communication aspects. This would have helped ID or capture Sam from the payroll record stealing if the staff has had better communication skills they would have known most if not all staff and pride a bit more when talking to him. Next will be the Goal-setting and planning, this would have helped the floor workers from accessing a website they should have not been on and not got the ransomware attack, for example if the workers have prepared the work day out and set goals to finish them plans they would have

been less likely to search for these sites. Also, a policy would have stopped them from doing that. Self-improvements will improve and make the staff member more confident and will help the company improve as well. Empathy should be in everyone's behavioural skills it shows that you can see their point of view for example if Jamie and staff around him had empathy they could see why they had to let him go and might have stopped the payroll stealing altogether. Finally, is the time management skill a very important skill to have, by having good-time management, the staff can organise the day around that and won't have to slack off and might miss a risk in the making. If the staff have a good set of behavioural skills and been trained in security awareness, they would have mitigated most of the risk that happened. Bodhih (2018) provide information for the visit.

Because behavioural skills are very attracting to others to do and follow their skills which can make toxic behaviour spoil the performance of the individuals and co-workers. It has been discovered that most people are not demotivated because of the work they need to do but because of the people they are working with, Jindal, Shaikh (2015) provide information for the visit. This would mean if the workflow is slowing down more staff around or change working partners to keep their morals high and keep an appropriate behaviour while at work lowering the risk of breaches.

Procedural Justice runs alongside the behavioural and security awareness training. Mainly because the way the work is set to be completed or how the company requires it to be completed. It is used on how to decide on what policies are established and created. It is meant to be fair and respectful. It is used to be neutral and based on fact. If a problem will arise in the company, what it already has the best thing to do is use the procedural justice to resolve it fairly and honestly to create a policy or procedures. Study.com (N/A) provided information for the visit.

2.2.3 Policies

Policies are the most critical sections of rules any company must abide by, if not they can be fined. Even though Rob has already introduced a policy which complies with the Data Protection Act (DPA), which is a promising start and has listed several other policies which he would like to be implemented, we will start with these first and branch out to cover more areas to make the company and staff more capable.

BYOD also was known as Bring your own device Policy. This type of policy has quite recently become more popular as everyone has a smartphone, tablet, and laptop. By maintaining this policy in place, it will safeguard the security of the network, because in the policy it will maintain the rules on what the staff can and can't access on their devices, by having a login system through the Wi-Fi. It will require the device to go through a firewall which will prevent any malicious attacks from getting through. In the scenario Rob had said people with improper mobile devices will be given an android device with a 6-figure pin which will also help the security of the network and sensitive information. Even if the staff are a diehard Apple fan, they will have to use the device for the wellbeing of the company.

The next policy listed is the information security education and training, this will line up with the training section of this report, making sure all staff members have been trained in security awareness and keep their credentials up to date.

Next, if the staff leaving the company policy (& other HR issues). This would have been very important during Jamie's resignation. The policy could have rules asking to hand in the ID Card one left the company, make sure no angry messages are posted on Facebook or LinkedIn until they have officially left the company. The HR issues can be included in this policy and once an employee leaves the company their account should be shut down and not allowing them to gather sensitive data.

The last one on the list was a proper risk analysis of the company's assets. The most effective way to control these is to apply for a copyright on the assets and audit the company every month, for example, to see if inventory has gone missing.

Another policy which can be implemented is the ISO 27k series. By complying with the ISO 27k mainly 27001 and 27002, which will help beef out the policies of the company. A positive complying with the 27K series is to make sure the company can run under the rigorous standards and if it can, then the company can apply for the ISO 27K certificate and can conduct more business with the government to show they are following the standards they need to. Just listing some of the policies and procedures, security policy, organisation of information security, HR security, Assets Management, Access control, cryptography, physical and environmental security, operations security, communications security, information systems acquisition, development, maintenance, supplier relationships, information security incident management, information security aspects of business continuity and compliance. To make sure the company follows these the management will have to get certified in these areas which will come from the training section. The ISO 27000 Directory (2013) provided information for the visit.

If the company does not what to use the ISO 24k series standards they can just employ the policies within the series. Since policies are kind of a living document that should grow and adapt with the company, even if the core meanings of the policy remain the same the details should change with the organisation. Gasior (2017) provided information for the visit.

3. Part 3

3.1. Introduction

This section is Part 3 and will discuss the ethical and moral issues of using human behaviour analysis and modification techniques within the organisation all of these will be supported by research and reading in this area.

3.2. Ethical Issues

Ethical issues are well-founded rules of standards of right and wrong. Which are mainly created and based from other people and are governed by professional and legal guidelines. Most if not all ethics come from certain communities and or social settings. Since Watson's Widgets has recently had an over hall of the policies, software, and hardware needed to mitigate attacks. The company from the beginning would have had a company culture which would have included the ethical issues and since the organisation has upgraded they will have to look at that culture and ethics to mould it into the new system of working. By doing this it will help mitigate attacks if everyone is on the page and knows the ethical issues the organisations what to follow. Jasuja (2012) provided information for the visit.

Many professional bodies will have codes of ethics, they are there to show how employees should work when in a professional setting. The staff at Watson's Widgets can apply to these bodies, which could have with ethics in the workplace and future employment showing that they are interested in this issue. Some of these bodies include the ISSA (information systems security association), IEEE, BCS (the chartered institute for IT), GIAC (global information assurance certification). They are many different bodies for each kind of job occupation, for example, IT and law will have different ethics when in the workplace.

Some authors said have discovered that there are three major themes of ethical decision making in the workplace, the first is ethical self which is more on the moral side of the issue, the second is malleable ethical standards which means the individual ethics can be moulded and changed depending on the situation, then finally is submission to authority meaning they will do what the high ups want even if it is against their own ethics. Li (2011) Provided information for the visit.

3.3. Moral Issues

Moral issues are very similar to ethical issues, but moral issues use the dos and don'ts, that fact shows the differences between ethics and morals as morals are ultimately an individual compass of the right and wrongs, people can get these from individual beliefs, for example, higher covenant such as religion, political affiliation, and culture norms. Morals are not a rules-based system like ethical issues. Since everyone is different we all have different moral issues, but when working in a company like Watson's Widgets ethical issues must be first and override the moral issues as it might go in contradiction of the organisation's goals. Diffen (2012) provide information for the visit.

But morals can also help a company in terms of competition for a raise or a promotion, some staff members might not have the same moral code and might be using immoral or unethical behaviour to gain a leg up, this should not be ok, and the ethics of company culture and policy should stop these types of behaviour. McFarlin (N/A) provided information for the visit.

4. Conclusion

In conclusion, the framework for analysing the breach is very good if it is a singular attack. But another type of framework should be used if more have occurred. Which they did in this instance. It shows how important training courses, behavioural attitudes, procedural processes, and policies are critical in running a modern business in 2018 - 19. All of the points will help in mitigating future attacks to the company, make sure the staff knows what to do if anything out of the normal happens and keeps the security of the company up to date which will also lower the running cost over time. It also shows ethical and moral issues will always be an issue with human workers and just needs to run effectively, to keep the company running smoothly from in-house disputes to outside attacks.

5. References

- 27000.org (2013) *introduction to ISO 27002 (ISO27002).* Available at: http://www.27000.org/iso-27002.htm (Accessed: 4 January 2019).
- Bodhih (2018) *Importance of behavioural skills training at workplace.* Available at: https://www.bodhih.com/behavioural-training/ (Accessed: 4 January 2019).
- Gasior, M. (2017) *How regularly reviewing policies and procedures is a key part of your organisations success.* Available at: https://www.powerdms.com/blog/why-it-is-important-to-review-policies-and-procedures/ (Accessed: 4 January 2019).
- Jasuja, N. Sehgal, P. Tilahun, A. Jain, S. (2013) *Ethics vs Morals.* Available at: https://www.diffen.com/difference/Ethics_vs_Morals (Accessed: 5 January 2019).
- Jindal, P. Shaikh, M. (2015) 'A study of behavioural training as talent management strategy in organisations'. *Universal journal of management,* 1, 1-6.
- Li, J. Madsen, J. (2011) 'Business ethics and workplace quanxi in Chinese SOEs: a qualitative study'. *Journal of Chinese human resources management,* 2, 83-99.
- McFarlin, K. (N/A) *Moral;s or ethics in the workplace.* Available at: https://smallbusiness.chron.com/morals-ethics-workplace-11363.html (Accessed: 5 January 2019).
- Rees, R. V. (2008). Clarity in the usage of the terms ontology, taxonomy and classification. *American Society of Civil Engineers, 20, 443.*
- Saceanu, R. (2016) *The importance of security awareness training.* Available at: https://www.smarttech.ie/news/importance-security-awareness-training/ (Accessed: 3 January 2019).
- Salas, E. Tannenbaum, S, I. Kraiger, K. Kimberly, A. Jentsch, S. (2012) 'The science of training and development in organisations: what matters in practice'. *Psychological science in the public interest*, 2, 74-101.
- Scamwatch (2018) *Showing stats for 'ransomware & malware' for '2018'.* Available at: https://www.scamwatch.gov.au/about-scamwatch/scam-statistics?scamid=33&date=2018 (Accessed: 1 January 2019).
- Tiwari, A. (2018) *What id social engineering? What are different types of social engineering attacks?.* Available at: https://fossbytes.com/what-is-social-engineering-types-techniques/ (Accessed: 1 January 2019).