International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 06 June 2024, pp: 1115-1121 www.ijaem.net ISSN: 2395-5252

A Cyber Security Case Study on eBayData breach

Nwosu Amarachukwu Grace

Date of Submission: 20-06-2024 Date of Acceptance: 30-06-2024

ABSTRACT: This report is an overview of some basic security associated services,that guard against risks to security of a system, using the ecommerce trading platform eBay February 2014 data breach, as case study. It covers some security policies, that not only detect the risks, but also outlines the conditions for a guaranteed protected system. Security procedures spot and stop incidents, therefore evaluating the security of a system demands an awareness of the procedures that implement the securitypolicies. Correspondingly, basic knowledge of certain theories and trust, which lead to the risks and the extent to which they may likely be executed, is equally required. Human beings are the most vulnerable link in the security procedures of any system, and so should be taken into account while establishing policies (Matt Bishop, 2002).

I. INTRODUCTION:

Computer security deals with computer associated assets.it could simply be defined as mechanisms used to ensure confidentiality, Integrity, and availability of information system. This includes hardware, software, and information being communicated, managed and saved. Information is key which is why big organizations like Marriott, Google, Amazon, eBay and many more are often the major targets of cyberthieves. This report will be discussing the February 2014, eBay data breach; the methods used by the hackers to breach their system, their intentions, the vulnerabilities that may have led to the breach, and the countermeasures taken by eBay to reduce the damage. It will also reflect what eBay did right or wrong and how they were able to resolve the breach.

eBay is an American international e-commerce business established by Pierre Omidya, in September 1995, and has its headquarters in San Jose, California. The business arranges a client-to-client retail sales via online marketplace, and is used by organizations, individuals, and governments to trade and acquire items. In 2014, a group of hackers got access to the login identifications of three of eBay's employees, providing them entrance to the internal network of the company.

II. LITERATURE REVIEW:

In recent years, the fundings in security changed from inessential to vital, organizations everywhere in the world now realize how important it is to constantly plough money into security (Yuri &Erdal, 2022). Every single data breach, cyberattack, vulnerability and exploit, deals with at least one component of the CIA triad; Confidentiality, Integrity, and Availability. The CIA triad is otherwise known as the three principles of Information Security or the CIA Model (Weissman, 2021). All cybersecurity process and mitigation practice, will also deal with one of the components on the minimum.

Whereas Confidentiality is concerned with restricting who can view a file or message, often achieved through encryption, Integrity is concerned with ensuring that the message or file has not been altered, either inadvertently or maliciously, and is often achieved through hashing. Availability is concerned with ensuring that networks and systems remain operational, so that approved users can have entrance to them, and it is often achieved through load balancing mechanisms and fault tolerance (Weissman, 2021).

In February/March 2014, ecommerce trading platform eBay, suffered a serious data breach which affected 145 million users, apparently their entire user base at the time. Customers' details like, email addresses, physical addresses, phone numbers, and encrypted passwords were exposed in the breach. eBay was compelled to ask all 145 million customers to change their passwords.

The organization was criticized for the vulnerability and also for the delays in communicating their customers. The breach was believed to have occurred more than a month before the organization made their first public announcement, requesting customers to change

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 06 June 2024, pp: 1115-1121 www.ijaem.net ISSN: 2395-5252

their passwords. Their employee log-in credential was compromised sometime in late February of 2014, enabling the thieves access to their user database. However, eBay established that they only discovered the compromised login roughly two weeks prior to their public announcement on May 21st ,2014.

The organization confirmed that the financial information of their customers, was however, not exposed during the incident as it could have worsened the whole situation. This does not dispute the fact that the stolen personal information of their customers, could still be sold to some criminals, who could in turn use them to commit crimes like impersonation, identity theft, and many more associated crimes. eBay's statement announcing the compromise, was first posted on their corporate website:eBayinc.com, which was believed to be a less trafficked medium, hence attracting an even bigger criticism, given that the affected customers are most likely not going to see the post. It is only a day later, that an announcement was made on behalf of the company, on their main website with very little information as just requesting customers to reset their password. This has left many in curiosity as to what exactly had happened.

The Commissioner of Information, UK, alongside the European data authorities, are working with a prospect to act against eBay concerning the breach. A few states in the US, are also investigating the theft of the personal information of up to 145 million clients. Meanwhile, several customers recounted troubles at the time of attempting to reset their passwords. eBay told BBC, that they are unaware of any technical troubles, associated with password reset malfunction on their site. However, they accepted that the site is engaged, and promised that the device for password reset is working. The company stated that they sent out millions of passwords reset emails to their clients, and also cautioned them that such emails do not contain any links. UK's Information Commissioner, speaking on BBC radio 5 live, said that the attack on eBay is very serious but the Office of the Information Commissioner cannot start an investigation immediately, because of some antiquated and intricate data protection laws. They would have to primarily interact with the data protection in Luxembourg, which is where eBay has its European headquarters. Millions of UK citizens were disclosed to be impacted by the breach.

Hugh Boyes from the institution of Engineering and Technology, queried why eBay kept that much data in the first place. UK Commissioner of Information, points out that companies ought to keep the smallest essential information.Thus, why do eBay require to store information such as addresses, and dates of birth of customers. As someone who uses eBay sporadically, he is worried that the company has lost his phone number, home address, and date of birth among other things like his email, username, and password. From an identity theft perspective, the breach is very serious as the thieves, have enough information to pose as an individual whom they are not, when trading with financial organizations.

Someone may ask, why should anyone be bothered about computer and network security? Compared to terrorism, risks of computers and networks may seem so light, however an average individual is most likely to be a target of cyberattack, than they are to be a victim of terrorism(Arthur et al., 2018). Organizations did not run businesses through the internet decades ago, as such ideas only existed as dreams in science fiction stories. Nowadays, millions of organizations run their daily businesses online. They depend on the internet to function, and handle their business. Huge sums of money are moved through networks, by means of bank transactions or credit card purchases. Anywhere there is huge sum of money, there are also individuals who will like to utilize that situation to steal or perform fraud.

Several years back, computer security was particularly concerned with basic components that form the computer. Many years ago, computers used to be the priceless items organizations could not bear losing. Currently, computer equipment is cheap in contrast with the information processed by the computer. The priceless item, went from the machine, to the information it keeps and processes. Extensive computer criminal actions many years back, was targeted towards obtaining illegal access to computer systems, not for the purpose of causing harm,but on a pursuit of academic inquisitiveness. The universal disposition of networks and computers, has reduced the supposed essence of breaching computers to acquire more knowledge about them. Therefore, it is normal today that malicious intents have substituted academic inquisitiveness.

For instance, sometime in 1995, Kevin Mitnick was detained over activities carried out in his computer in 1980s and 1990s. Itinvolves unlawful access to about 20,000 credit card numbers, which included some belonging to Silicon Valley moguls,thereby causing serious

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 06 June 2024, pp: 1115-1121 www.ijaem.net ISSN: 2395-5252

millions of dollars damage to computer operations. He pled guilty to two counts of computer fraud, four counts of wire fraud, and one count of tapping wire communication illegally. He also acknowledged obtaining illegal entrance to computer systems of organizations like Sun Microsystems, Motorola, and Novell. He explained how he used diverse sets of tools and methods, which includes social engineering, replicated cellular telephones, and sniffers. However, there was no indication that he used the files he had stolen for financial gain, and would back his actions as inoffensive kind of play.

A second example is the slammer worm which was released to Microsoft by researcher David Litchfield in July 2002, and submitted with the consent of Microsoft at a Black Hat security conference held in October 2002. It is a 2003 computer worm that caused a denial of service on some internet hosts. It utilized a buffer-overflow weakness in computers running on Microsoft SQL Server. The worm had already infected 120,000 hosts on the minimum within the first 24 hours of its release. It caused network outages and interruptions of airline flights. It is projected that it took less than 10 minutes for the worm to corrupt up to 90 percent of the hosts, and doubled the number of affected hosts every 8 seconds.Ensuring that software is current with regards to release from seller, is one of the efficient methods security professionals can utilize to tackle incidents on their computer networks and systems. Impact of worms and virus outbreak would not have been acute if everyone had implemented security update patches just as soon as they were released.

On April 9 2009, San Jose area of California was hit by internet outage and widespread phone disconnection. The outage however, was not an outcome of cyberthieves bent on getting illegal access to computers and networks, rather, it was an outcome of numerous cuts in the fiber optic cables that transmit signals. The vandalization caused a loss of the entire telephone and internet service for thousands of people in the San Jose area. Now, when a computer is unable to do what it is expected to do, it is believed not to be secured. In like manner, Information Security is described by the information actually secured from illegal access or modification, and at the same time accessible to authorized individuals when needed. In the past, risks were relatively smaller and commonly irritant, but subsequently, more structured components of cybercrime have sufficed. The cyber threat prospect became more alarming with latest enemies out to execute operations like exploiting systems with aim to gain financially, steal intellectual property, or even financial information such as the PII (Personally IdentifiableInformation). The APIs (Advanced Persistent Threats) illustrate latest kind of attack models. Advanced signifies the adoption of complex methods such as spear phishing as a transmitter into a victim. Persistent signifies the enemy's aim of setting-up a continuing seclusion on a system. Threat signifies intention; exploitation. A lot of APIs can carry on for years in a system and remain undetected the entire period.

From an academic viewpoint, the first versions of ransomware date back to mid-1990s to late 1990s and so is not an unfamiliar threat. However, it was not until recently that it was utilized, so was practically hypothetical. Ransomware is rated as one of the highest threats nowadays as it has consistently developed since 2012. Remarkable number of recent ransomware attacks make use of a hybrid encrypting scheme, locking up records on the computer of the victim until a ransom is paid. In May 2017, WannaCry spanned as an encrypting worm, striking Systems that operate Microsoft Windows yet to be patched against SMB (Server Message Block).

III. DISCUSSION AND ANALYSIS:

In 1991, a model framework used for creating and assessing information security programs, in what is known as McCumber Cube was created by John McCumber. The security model is portrayed as a three-dimensional cube-like grid which is comprised of:

- Information security properties: this is the first dimension of the model, and comprises of the three things that make up the Information security; Confidentiality, Integrity, Availability. For example, in the eBay 2014 February attack, the Confidentiality principle was violated as personal details of over 145 million clients, got exposed to unauthorized persons; the cyberthieves who managed to gain illegal access to the organization's network.
- Information states: the second dimension of the information security model, consisting of Processing, Storage and Transmission. Information can be conveyed through the internet or network and can also be saved on a hard drive. One may ask why eBay stored that much data of over 145 million clients including encrypted passwords, phone numbers, and home addresses on their database. They could easily have used any

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 06 June 2024, pp: 1115-1121 www.ijaem.net ISSN: 2395-5252

other storage means if they must keep such massive data.
- Safeguards: technology, is not necessarily what Information Technology Professionals consider when planning solutions to the information security problem. Rules and Methods offer the foundation for an organization.

How would one know how to configure their firewall without the appropriate rules and methods to direct them? It is a complete must, to teach employees to be security aware, so that whatever security measures executed in the organization will be successful. The operational model of a computer security, comprises of diverse technologies. Protection, is the entirety of prevention, and the measures used for detection and response (Ahmed, 2020). Controls need to be applied at diverse points before security can be effective. For instance, an organization may decide to get a security guard to watch the outside and at the same time may also require a biometric palm scan before accessing the server room. Access control describes the level of security structures that can be used to stop unapproved access to network or computer system. A lot of devices can be configured in a way that clearly specifies what kind of access or privileges a user has at a particular given time. For example, just because a particular employee, has access to log onto the organization's network, does not mean that such employee also has the permission to use maybe the printer. Authentication confirms that a user is actually whom they say they are; confirms the identity of a user. The user might need to generate a password, biometric like fingerprint or a card.

Communication security has various segments like:
- Emission security: comprises of actions taken to preclude unauthorized persons from interrupting or examining electronic waves a machine may generate.
- Transmission security: measures taken to ensure transmissions are protected from interception.
- Cryptosecurity: this makes sure that cryptosystems are secure and correctly used.
- Physical security: physical actions taken to protect confidential documents, data, and equipment.

Technology is not required for social engineering to take place; all the attacker needs to do is to convince their victim to provide their confidential information. Social engineering is one of the highly effective techniques cyberthieves use to gain access to networks and computer systems. In the attack on eBay, the cyberthieves might have used social engineering to deceive the employees into running their malicious file. Then again, there is also a possibility that they might have impersonated the employee by injecting undesired codes in their database. Social engineering collects what appears to be worthless bits of information, that when assembled disclose other sensitive information. Due care and Due diligence are the two terminologies that arise when examining steps taken to protect an organization's environment. Due Care examines all the measures an organization takes, in order to protect their company, their resources, and their employees. Due diligence demands that organization have recurrent actions to ensure that precautions are operational and sustained. Although eBay till date, has not disclosed how their employees' credentials were obtained by the cyberthieves, history has shown that most attacks start by web application vulnerability exploitation, or social engineering attack.The human side of computer security is secure system development and management.

Protection is not even automated in a reliable system; therefore, administrators require spelt out guidelines that distinctly defines what methods and actions to take earlier while working towards security.Security in this evolving world no longer depends on what our software or tools can do for us, rather in what we can do for ourselves. Setting security policies for our organization, and applying diligence in stating and sustaining them, is the first step in maintaining protection. This effortspans through all levels. While security Administrators are the ones in charge of implementing security polices with regards to protection, detection and enforcement, it is the responsibility of the user to ensure security is kept. The managers and proprietors must approve, sustain and penalize those who violate the process. For example, if the security policy of an organization requires that they regularly back up data, the administrator should make sure he trains users on how to do the backup and also severely punish them if they fail to comply.

Incident response is the most strategic area for all units to meet; what actions to take when there is a breach. In the eBay 2014 breach, one would say that the organization does not prove to have a good workable incident response. Considering the manner in which they handled the whole situation. It took over a month before the organization even noticed the breach. Even after

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 06 June 2024, pp: 1115-1121 www.ijaem.net ISSN: 2395-5252

they noticed, it took days before they reluctantly made a post on their less traffic site, simply requesting clients to change their password. eBay's response to losing control of over 145 million clients' information is said to be the worst form of response ever.Security policy is an existing record that needs to be efficient and regularly assessed. There are certain ways to interpret security policy into an actual defense: modifying and setting up intrusion detection systems and firewall, training users, administrating passwords, and assessing audit logs. Administrative security comes in 3 categories:

- Overall security administration and planning: this involves cooperating with management to establish a security policy for your organization, circulate it, get management approval for it, carryout risk analysis and disaster planning, educate users and supervise employees.
- Daily security administration: this category involves creating account and allocating security profiles to users. Some controls may include how often they are permitted to change their passwords, and at what hours they are free to log in.
- Daily system administration: involves making sure the system is running, performing backups on a daily basis, scanning for breaches, and assessing the state of both the software and hardware used in operation.

Computer security is a deal so once you are thinking of operating, developing or purchasing a security product, you have to contrast its cost to the risk of forgoing it. Great number of organizations normalize this practice and call it risk analysis. Risk analysis is a method used to assess possible deficits that may ensue from system weaknesses, and to measure the loss that may occur should any risk happen. The paramount objective of risk analysis is to choose an economical but efficient safety measures to cut risks to tolerable degree. Fundamentally, risk analysis is simply a means to fathom how valuable your system is, and the extent you are prepared to go with regards to people, tools, and finances to guard it (Lehtinen et al.,2006). A regular risk analysis requires observing all your physical resources such as buildings, tools, and computers and deciding how to safeguard them. The most valued resource one's organization has may be the data processed by their computers, consequently, one has to think of safest way to safeguard it. When assessing the data resources of your organization and reflecting if to safeguard it, and how to safeguard it, you would require to ask yourself these questions:

1. What data do you have and what is their importance?
2. How unprotected is it?
3. What will it cost to protect it?
4. What will it cost if it is lost or endangered?
5. Who will you call should there be an attack on your system?

Planning for disaster is one of the most essential things one can do to guard their organization from calamity. Disaster recovery plan is a preparation, that helps in maintaining the accessibility of your data and computer in occurrence of a disaster. The disaster plan may include actions such as backups and prearranging for other facilities. It could be formal or informal. Informal is when you make a mutual arrangement with another organization, branch or section to use one another's things in case an attack happens. Formal is when you prepare a distinct place for backup or outrightly outsource to organizations who handle disaster preparation.

Security specialists alerted that the clients' information that were stolen will most likely make eBay clients phishing targets effortlessly. The cyberthieves can send emails with malicious links and entice their targets into clicking such links. They can also lead them to fake login displays where they are requested to input more important information like their social security number or password. eBay communicated the Federal Bureau of Investigation's San Francisco office and also an external Computer Forensic Firm. Collaborating, they discovered that the cyberthieves had been in their corporate network since late February. eBay found through their computer logs, that the thieves had taken the identification of some of their employees and obtained illegal entry into their corporate network allowing them to duplicate a database which contained information of over 145 million clients. eBay informed their customers who use same passwords for their PayPal to get a new one straightaway. Although laws of notification vary by states, some states need organizations to inform customers of an attack only when their names, social security number, and credit cards are jointly compromised. However, encrypted information is exempted.

In eBay's case, the company encrypted the passwords of their clients, but left information such as their names, email, birth dates and physical addresses in plain text. A high number of states, would not have demanded eBay to reveal the

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 06 June 2024, pp: 1115-1121 www.ijaem.net ISSN: 2395-5252

breach. Some state like North Dakota, needs organizations to reveal an attack only in situations where a client's name is endangered together with their date of birth. Owing to the breach suffered by eBay in February 2014, a federal judge has dismissed the lawsuit filed against eBay. The lawsuit was filed by Collin Green sometime in July 2014, on behalf of American eBay users whose information were compromised during the breach. In the lawsuit, he alleged that the data breach caused financial harm for the clients but was unable to prove his claims. eBay maintained that there was no indication that payment card details had been compromised, or was there any actual damage suffered by any client and the ruling judge seemed to agree.

Information security is not restrained to wiredsystems, it is similarly crucial for wireless communications such as cellular andWIFI. Encryption is an essential technology in countless ways of communication. There is need to explore new improvements such as applications from algebraic formations like ECs (Elliptic Curves), rings and quantum physics. Over the years, standard cryptography has advanced to quantum cryptography, which is equally a branch of quantum information theory. Quantum cryptography is created on the quantum physics structure, and explains the difficulties of key distribution which is a critical section of cryptography that allows for data security. The key grants permission for coding of data, so that in order to decode the data, one should understand the key used in coding them. Encryption is coding a data using a key, and the reverse gradual decoding of the encrypted data is known as decryption. Encryption algorithm is in two phases; symmetric and asymmetric. Encryption of data makes data unusable and also stops the exposure of such data to unapproved access.

The three-dimensional approach required for data security includes: Detection, Prevention and Response. Information usually stays on storage medium that is often accessible across a network. The network is created with limits in it, such that each entry point gives a path for incoming and outgoing movement via the router, broadened by a firewall. Detection allows one to examine the actions of everyone using the network, offers a way to distinguish degrees of activities, and suggests likely evidence to network intrusions. Response is proportionately crucial, because a network intrusion should not bepermitted to reoccur. The three-dimensional approach is progressional, thus, system investigation and policies should be considered when designing a secured information network. Cryptographic protocols will allow protected interaction by addressing nonrepudiation, authentication, confidentiality, and integrity.

IV. CONCLUSIONS AND RECOMMENDATIONS:

One cannot assume a system is secured because it was created by them. Every man-made system is bound to have a flaw, and it doesn't take long before someone discovers it. Computers and the internets have changed virtually all outlook of our lives both professionally and personally. Safeguarding information is an essential issue for any organization;therefore, they should make computer security a priority.Why is computer security essential? It is essential because knowledge of computer security fundamentals can help prevent your information from getting into wrong hands.Delicate information is indispensable, and this has made computer systems bull's eye to cyberthieves and hackers. Computer security experts must make effort to incorporate best computer security approaches intheir organization. This includes overseeing computer and network security, and designing a security-oriented values in their organization.

There are various kinds of computer security that effect different sections of an organization's digital and physical arrangement. Security experts should concentrate on these forms of security: Network security, Application security, Endpoint security and Information security. Every single one of these kinds of computer security comprises of various elements and can most likely be studied as their own expert fields. Network security concerns the physical elements of a network like the Servers, Routers and the software elements like the firewalls and security policies. Computer security professionals need to be well informed on extensive computer security issues, so as to safeguard their organizations from the progressing cyber threats they are faced with on a daily basis. Computer security safeguards people and organizations from loss of essential information and cyberthreats.

REFERENCES:

[1]. Weissman, J (2021). Principles of Computer Security. New York. McGraw-Hill Education.
[2]. William Arthur (2022). Principles of Computer Security: CompTIA Security+ and beyond. (sixth edition). New York. McGraw-Hill Education.

[3]. Conklin,Wm.A. White, G, Cothren, C, Davis, R & Williams D (2018). Principles of Computer Security: CompTIA Security+ and beyond. (fifth edition). New York. McGraw-Hill Education.
[4]. Rishalin, P, & Mohammed, A (2023). Ethical Hacking Workshop. Packt Publishing.
[5]. Sabihi, Z (2018). Learn Ethical Hacking from Scratch: Your Stepping Stone to Penetration Testing. Packt Publishing.
[6]. Ahmed, F S (2020). CompTIA Security+ Certification Study Guide: Network Essentials. Apress.
[7]. William Arthur (2022). CompTIA Security+ (sixth edition). New York. McGraw-Hill Education.
[8]. Lehtinen, R, Gangemi, G, T& Russell, D (2006). Computer Security Basics. Sebastopol, California: O'Reilly.
[9]. Matt Bishop (2004). Introduction to Computer Security. Addison-Wesley Professional.
[10]. Matt Bishop (2002). Computer Security: art and science. (first edition). Addison-Wesley Professional.
[11]. John, R.V (2017). Computer and Information security handbook. Morgan Kaufmann.
[12]. Yuri Diogenes &ErdalOzkaya (2022). Cyber Security Attack and Defense Strategies. Packt Publishing.
[13]. Warwick Ashford (2014, May 23). eBay under fire over handling of data breach. TechTarget. https://www.computerweekly.com/news/2240221226/eBay-under-fire-over-handling-of-data-breach
[14]. Cyber Security Principles. (2023, Dec, 01). Australian Signals Directorate. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-principles
[15]. AkhilBhadwal (2023, Sept, 15). 14 Key Principles of Cyber Security to Follow. upGrad. https://www.knowledgehut.com/blog/security/principles-of-cyber-security
[16]. Stallings, W, & Brown, L (2017). Computer Security: Principles and Practice.(fourth edition). Harlow. Pearson EducationLimited.
[17]. Nicole, Perlroth (2014, May, 21). eBay Urges New Passwords After Breach. The New York Times. https://www.nytimes.com/2014/05/22/technology/ebay-reports-attack-on-its-computer-network.html
[18]. Krausz, M (2014). Information Security Breaches: Avoidance and Treatment Based on ISO27001.Cambridge IT Governance Ltd.
[19]. Matthew, J, Schwartz (2015, May, 5). eBay Breach-Related Lawsuit Dismissed. Bank Info Security. https://www.bankinfosecurity.com/ebay-breach-related-lawsuit-dismissed-a-8200
[20]. eBay could face compensation claims following cyber attack, warns expert.(2014, May,14). Pinset Masons. https://www.pinsentmasons.com/out-law/news/ebay-could-face-compensation-claims-following-cyber-attack-warns-expert
[21]. Troy, H (2014, May, 22). The eBay breach: answers to the questions that will inevitably be asked. Troy Hunt Blog. https://www.troyhunt.com/the-ebay-breach-answers-to-questions/
[22]. James Taylor (n.d), Security Breach at eBay. https://www.essaytyping.com/security-breach-ebay/
[23]. What is WannaCry ransomware? (2024). Kaspersky. https://www.kaspersky.com/resource-center/threats/ransomware-wannacry
[24]. Malia, Wollan (2009, April, 10). California: Vandals Cut Phone Cables, Police say. The New York Times. https://www.nytimes.com/2009/04/10/us/10brfs-VANDALSCUTPH_BRF.html
[25]. Learning the language of cyber security. (2017, Dec, 14). Capitol Technology University Blog. https://www.captechu.edu/blog/learning-language-of-cybersecurity
[26]. Robert S, & Ben, C (2024, January). Information Assurance(IA). TechTarget.https://www.techtarget.com/searchsecurity/definition/information-assurance
[27]. Robert, A (2014, May, 22). What can we learn from eBay Hack Attack. Invicti. https://www.invicti.com/blog/web-security/learn-ebay-database-hack-attack/