A Case Study of the 2014 eBay Data Breach: Analysis, Implications, and Lessons Learned

Student First and Last Name: Dawda Wally

Student ID: R2404D17931625

Date of Submission: 04th August 2024

Assignment Name: uel-cn-7016_assignment-1.

Module Name and Code: UEL-CN-7016-64360 Computer Security (64360)

Table of Contents

1. Title: A Case Study of the 2014 eBay Data Breach: Analysis, Implications, and Lessons Learned

2. Abstract

The 2014 eBay data breach is considered one of the key events in the field of cybersecurity given that it affected over 145 million customers. This report provides a critical analysis of the breach and the incident given the core principles of computer security; confidentiality, integrity and availability. It looks at the techniques used by the attackers and, the reasons why they conducted the attack. It also assesses the countermeasures that eBay put in place after the breach and the extent to which the same helped reduce the impact and strengthen the company's security posture. The findings show that enhanced security principles, effective stakeholder communication, policy, and regulatory compliance should be strictly adhered to at all times.

3. Introduction

eBay is a global leading e-commerce company which was attacked by hackers in February 2014. The security incident is considered one of the largest global cybercrimes. The security breach inflicted a blow to approximately 145 million customers and was one of the largest in the history of eBay. Such an incident pointed out that there are severe and inalienable flaws in the company's security shields and processes, and has provided important lessons for both eBay as well as other organizations in the computer security domain (Goodin, 2014).

eBay is one of the largest Internet market systems, based on the C2C and B2C business models. As one of the biggest international e-commerce platforms, a group of hackers explored eBay's security protocols intending to attack many customer accounts to steal sensitive personal data for nefarious purposes. During the breach, the hackers stole encrypted passwords and some sensitive user data such as names, addresses, dates of birth etc (Perlroth, 2014).

An issue that merits discussion is the fact that the breach was reported to have been discovered in the early parts of 2014, yet the firm only came out to address the matter in the middle of the same year which prompted many to question the firm's seriousness in handling of the situation. When the company released information about the breach to the public, there was strong criticism from customers and regulatory authorities regarding the company's authenticity in protecting users' data and the handling of the attack (Leyden, 2014).

Unlike similar cyber attacks, this one targeted a small number of eBay's employees through phishing. The credentials stolen were then used to gain access to eBay's internal network and to navigate the network till they got access to a large number of user data (Jakobsson & Myers, 2006) which resulted in reputational damage (Goodin, 2014). This breach also had other effects on different players in the eBay business inclusive of the investors who were worried about the security of eBay and its ability to address the already known cyber threats (Perlroth, 2014).

This report focuses on the examination of the 2014 data breach at eBay Inc. It explains the strategies used by the attackers and some of the justifications for the attack as well as the vulnerabilities exploited. The report also establishes the defensive steps eBay had taken after the breach. It further discusses the consequences of a breach to customers, stakeholders, eBay and in general, the implications of cyber attacks.

4. Literature Review

4.1 Fundamental Aspects of Computer Security

In this section basic concepts that are related to computer security are described in detail. These principles very fundamental in the protection of information systems against different threats. These aspects are discussed below.

4.1.1 Confidentiality, Integrity, and Availability (CIA Triad)

The CIA triad is recognized as one of the most widely used security models used to define the objectives of security and to evaluate the results of security activities. It consists of three fundamental components:

- **Confidentiality:** By the postulated principle, it means that only the people who are supposed to gain access to information should have access and that information should be securely stored at all times. Authorization, encryption, secure channels, etc, are the methods which Stallings (2017) states make information secure and confidential. For instance, the eBay leakage involved the usage of weak passwords which means that strong encryption mechanisms play a role in preserving users' information (Goodin, 2014).
- **Integrity:** Integrity can be described as the capacity to maintain the nature and content of the data and prevent anybody from changing it without permission. Having said this, it is also important to point out that several other general methods can be used for data integrity and they are: checksum, hashing and digital signatures (Gollmann, 2011). One needs to consider the aspect of data integrity that needed protection to prevent third parties from modifying users' data, which perfectly fits the case of eBay data breach.
- **Availability:** It asserts that information should always be available when authorized users require it. This principle is sometimes known as the administration tools and equipment, renewal of systems and the existence of backups if the system breaks down (Pfleeger & Pfleeger, 2012).

4.1.2 Authentication and Non-repudiation

Authentication and non-repudiation are critical components of computer security that ensure the legitimacy of users and actions within a system. Authentication and non-repudiation are among the significant subcategories of computer protection that guarantee the credibility of the subjects and their actions.

- **Authentication:** This one genuinely verifies the accuracy of the user or system with a view of only granting access to the right entities. The most commonly used categories include passwords, biometrics and multi-factor authentication as highlighted by Menezes, van Oorschot, & Vanstone (1996). The eBay attack revealed that it is high time for more secure methods of authentication as hackers are continuing to gain illegal access to computers, and sensitive data among other important assets.
- **Non-repudiation:** It is the property which ensures that a party cannot dispute having acted. Encryption/decryption can be applied to other functions as needed while digital certificates and logging of events are used for non-repudiation (Kaufman, Perlman & Speciner, 2002). Regarding non-repudiation, which was not a problem in the eBay scandal, one realizes that non-repudiation is a critical element to ensure that people can be held accountable for their actions in cyberspace (Brooks et al., 2018).

4.1.3 Common Security Threats and Mitigation Strategies

Understanding common security threats and their mitigation strategies is essential for developing a comprehensive security posture. This section focuses on the conventional notion of threat agents as well as precautions that can be taken to arrive at better guidelines for policy formulation in addressing security threats.

- **Malware:** Malware is a type of security threat in which a virus, worm or ransomware is designed to harm or infiltrate computer and network systems (Brooks et al., 2018) . The precaution techniques that have been deemed to be efficient in the fight against malware include the use of anti-virus programs, frequent updates to systems, and increasing awareness of the end users (Symantec, 2018). Malware did not directly lead to the eBay breach but understanding the kind of threat malware is can help one to have a wide vision of cybersecurity risks.
- **Phishing:** Phishing is quite more structured as it is carried out through fake emails or messages. The attacker will attempt to persuade the user to give out his or her password or any other account details. Some of the measures that have been proposed to counter phishing attacks are: raising awareness among users and the utilization of improved

technologies in the identification of phishing attacks (Jakobsson & Myers, 2006). Of course, the nature of the incident that happened was a so-called phishing attack, and this fact confirms the efficacy the proposed measures would have had in preventing the data breach (Brooks et al., 2018).

- **Denial of Service (DoS) Attacks:** Like other types of cyber attacks, DoS attacks majorly target the networks' resources. Some of the measures that can be taken are firewalls, intrusion detection systems, etc. (Stallings, 2017). Although this type of attack did not apply to eBay's case, it is however important to recognize DoS attacks and ways to effectively prevent them so the CIA triad of organizations' systems are not affected.

4.2 Security Frameworks and Standards

Security frameworks and standards consist of approaches and techniques to combat security threats within cyberspace. There are two most popular frameworks, these are the NIST Cybersecurity Framework and ISO/IEC 27001.

- **NIST Cybersecurity Framework:** The NIST Cybersecurity Framework is a framework of guidelines which when implemented can help mitigate risks, prevent attacks and protect assets within organizations (NIST, 2018). The core features of the framework include implementation Tiers and Profiles that help organizations understand and manage their cybersecurity risk and allow them to improve their security posture.
- **ISO/IEC 27001:** The ISO 27001 series focuses on information security management systems (ISO, 2022). The standard contains risk management, risk mitigation, risk prevention, and risk identification as well as methods that could be used to constantly improve the protection of information and information systems.

4.3 The Role of Human Factors in Cybersecurity

Human factors play a significant role in cybersecurity, as human errors and insider threats can lead to security breaches. Human factors are deemed to be important in cybersecurity since

employees may be potential threats; this is in the context of insider threats as well as through inadvertent human errors that lead to security breaches.

- **Human Error and Security:** One of the critical aspects that are inherent to all organizations is the human factor leads to security incidents, and it is estimated that most of the security issues arise out of the fact that individuals in the organizations do not receive adequate security training or are even unaware of the measures they should take to prevent security incidents (Bosworth, Kabay, and Whynem, 2014). Phishing and social engineering are some of the classes of attacks that are mostly executed using human weaknesses and /or human flaws. As a result of the findings of the eBay breach, it is recommended that there should be proper training and the creation of awareness regarding the use of technology especially in organizations.
- **Insider Threats:** These are the activities that are probably performed within an organization either intentionally or inadvertently (Greitzer & Frincke, 2010). These threats in a more negative meaning can be potentially lethal in the sense that they mean leakage of information or even sabotage of the organization by employees with malicious intent. It is possible to prevent Insider threats by applying methods such as Access Controls, Monitoring, and Behavioral Analysis (Bosworth, Kabay, and Whynem, 2014).

4.4 Evolution of Cyber Threats and Defenses

The cybersecurity landscape is continually evolving, with new threats and advances in defensive technologies emerging regularly. Cyber security risks are genuine and evolving, that is, new risks or forms of the existing dangers or innovations in the tools used to counter them are developed from time to time. Some of these are discussed below.

- **Emerging Threats:** Threats within cyberspace are not fixed but constantly evolving, and new ones including ransomware and advanced persistent threats or APTs are being discovered (Symantec, 2019). New threats can be studied to obtain useful information about their nature and this way, amendments to the security policies and measures for defence should be instituted.

- **Advances in Defensive Technologies:** The technologies used in defensive measures have also advanced due to the existing threats. This involves the application of Artificial Intelligence (AI) and Machine Learning (ML) in threat identification (SANS Institute, 2020). Another area in which using AI for security purposes is beneficial is that of big data processing and pattern identification and shifts that expose symptoms of risks. The nature of the threats in the cyber domain is evolutionary and thus it's imperative to continuously build up the capability to counter them (Bosworth, Kabay, and Whynem, 2014).

4.5 Overview of the 2014 eBay Data Breach

The 2014 eBay data breach serves as a critical case study for understanding the impact of security lapses and the importance of robust cybersecurity measures. That is why the case of eBay Corporation's data breach that occurred in May 2014 is an excellent example to study the consequences of such failures and the significance of having efficient cybersecurity programs in place.

- **Background on eBay:** eBay is a company that was founded in 1995 and it is an online business platform through which different market actors interact. Since the present website is attracting tens of millions of active users, it is among some of the largest brands that attract cybercriminals to perform their activities. That is why an attack on the company's extensive database of personal and financial information interested cybercriminals.
- **Details of the Breach:** The cyber attack referred to in this case is the eBay cyber attack that took place in February 2014 where attackers succeeded in getting through the network of the firm phishing. The criminals obtained usernames and passwords, which led to the invasion of eBay's intranet and user data database. This led to the exposure of some details of users including their encrypted passwords (Goodin, 2014). Although this data breach occurred in the first half of the year, eBay took too long to reveal the incident to the public and only reported it in mid-year, more specifically May of the same year and this action was frowned upon (Leyden, 2014).

- **Impact of the Breach:** The consequences of the breach on eBay were identity thefts of the clients and loss of the company's reputation. Measurable criticism was meted out to eBay after the firm had responded slowly and after the completion of the first phase of the security measures (Perlroth, 2014). The case made it possible to understand real-life lessons of eBay's inability to have a strong security check with the need for organizations to have proper security.
- **Initial Response and Public Disclosure:** The initial actions that eBay first took were to notify the users of the corporation to change their password and also conduct an investigation within the organization. The time taken to manage the breach and to notify the public of the incident was criticized to have been poor and unresponsive (Ebay Inc., 2014). The breach showed effective and timely communication and responsive event management is crucial during and after cyberattacks.

4.6 The Psychology of Cybersecurity

Understanding the psychological aspects of cybersecurity can provide insights into how users and attackers think and behave. Psychological factors are often associated with the sphere of cybersecurity, and knowing about them can enhance one's understanding of the user and the attacker's psychology.

- **User Behavior and Compliance:** Some of the user's compliance with the security policies in the present study carry over residual psychological factors including perceived threat and response efficacy as put forward by Pfleeger (2012). Thus, any effort to enhance their knowledge will go a long way in enhancing the level of compliance with the existing security rules and regulations.
- **Social Engineering:** Some of the often-used principles in social engineering attacks are trust, authority, and urgency which are used by the attackers to infiltrate networks and computer systems (Hadnagy, 2011).

4.7 Legal and Ethical Considerations in Cybersecurity

Cybersecurity practices must align with legal and ethical standards to ensure compliance and protect user rights. Therefore, it is highly pertinent to regard the legal and ethical standards of the organization to prevent the violation and to adhere to the users' rights.

- **Data Protection Regulations:** For instance, some of the regulations are laid under the General Data Protection Regulation (GDPR) of the European Union (EU) on how personal data needs to be dealt with (European Union, 2016). The guidelines outlined should be strictly adhered to so as not to incite legal implications.
- **Ethical Hacking:** Ethical hacking involves the legal hacking of a system to expose its flaws, and on some occasions coming up with a possible remedy to the identified vulnerabilities (Kim, 2018).

4.8 Cybersecurity Education and Training

Education and training are vital for developing a skilled cybersecurity workforce and promoting a security-conscious culture. Education and training are effective instruments for the certification of eligible human capital for cybersecurity support and enhancement of people's awareness of various cybersecurity issues.

- **Training Programs:** Adequate training of employees can be useful to minimize the occurrences of security incidents due to errors made by the employees in a given organization (Pfleeger, 2012). Hence, employees should undergo training now and then so that they can be informed of the existing threats and protective measures to counter those threats.
- **Certifications:** Some of the most popular well-known ones are the Certified Information Systems Security Professional (CISSP), and the Certified Ethical Hacker (CEH); these are the certifications that point to the competence of an individual in the sphere of cybersecurity (ISC2, 2020).

5. Discussion and Analysis

The present section provides a critical evaluation of all the aspects of the 2014 eBay data breach.

5.1 Computer Security Issues Related to the Breach

5.1.1 Methods Used by the Hackers

The 2014 eBay data breach involved several methods that underscore the evolving nature of cyber threats. Here are some of the main tactics that were prosecuted in the 2014 eBay data breach. They are described below to indicate the dangerously evolving nature of cyber threats and how these apply to eBay's data breach.

- **Phishing Attack:** The attackers launched a slightly more complex procedure to capture or obtain the eBay employees' credentials. Unfortunately, phishing continues to be efficient and widespread in cyber threats because it compels users to compromise information and provide seemingly genuine authorization to the attackers (Brooks et al., 2018). In this breach, the technique that was used to initially get into eBay's network was done by running a phishing scam.
- **Privilege Escalation:** Through the granting of higher access rights, attackers were able to move through eBay's network after gaining first entry into their computer systems. Privilege escalation assists the cyber attackers in transitioning through a network plan because the higher privilege level unfolds vulnerabilities (MedeAnalytics, 2015). This also helped the attacker to use lateral movement to acquire encrypted users' data.

5.1.2 Intentions of the Hackers

Understanding the motivations behind cyberattacks can provide insights into preventative measures. This section explains the motivations of the cyber attack and offers some possibilities on how these could be dealt with.

- **Financial Gain:** More specifically, this breached data which included more explicit personal information could be used to make money through identity theft. As

aforementioned, the aforesaid data is beneficial for criminals for impersonation, embezzlement or to put the data up for sale on the black markets as stated by Perlroth (2014). Unfortunately, such factors as money are among the necessities often at the root of cyber criminality, thus, a constituent of an organisation should ensure that such crucial information receives appropriate safeguards, as well as constant security updates and assessment.

- **Exploitation of Weaknesses:** The attackers infiltrated eBay's system through vulnerable entry points, thus, having an unprecedented chance to annex as many people's data as possible. However, their primary aims included other unlawful actions (Goodin, 2014). While security is supposed to be checked occasionally, vulnerabilities are supposed to be attended to constantly since it is acutely predicted that threats in the cybersecurity domain are not constant.

5.1.3 Vulnerabilities Leading to the Breach

Several vulnerabilities contributed to the breach, revealing critical gaps in eBay's security posture. The following weaknesses gave the intruders easy access to the company's systems and exposed some of eBay's most pertinent shortcomings when it comes to security.

- **Inadequate Employee Training:** What made the phishing attack possible was a general lack of strict rules, precautions, and procedures associated with cybersecurity threats among employees in the organization (Chapple, Stewart, and Gibson, 2018). Training activities are therefore important in raising awareness on the part of the workforce on aspects relating to phishing attacks (Symantec, 2018) because even the best and most secure technologies are not invulnerable to penetration through the human factor.
- **Network Security Gaps:** It can be concluded that network security was not sufficiently effective to prevent lateral movement inside eBay's network. This emphasises how there was a need for proper internal network segmentation and monitoring to be in place (Pfleeger and Pfleeger, 2012). New measures in conjunction with the network security means are needed to decrease the overall impact of the break-in and to limit or control accesses; this is a testimony to the need for a multilayered approach to security.

- **Delay in Detection:** The event continued for a few months after the defunct server was detected showing inadequacies in intrusion detection and monitoring systems at eBay. The monitoring aspect and generation of real-time alerts are very useful in identifying any suspicious acts that may be going on (Leyden, 2014). This underscores the importance of improving security intelligence to reduce the time that elapses before threats are identified.

5.1.4 eBay's Post-Breach Countermeasures

In response to the breach, eBay implemented several countermeasures to address its vulnerabilities and enhance its security posture. Some of these are:

- **Password Reset:** eBay advised all its users to change their password after the incident. The motivation here was to avoid a repeat of a situation where customer accounts are compromised and as such regain the trust of the users (Par Server, 2014). A change of passwords is probably applied in such contexts where the breach involves theft of the authentication parameters.
- **Security Enhancements:** They created a situation where other aspects of security had to be reviewed better and other components of security had to be made even better through encryption and Identity and Access Management (Ebay Inc., 2020).
- **Increased Transparency:** In the above discussion, the company was in a position to communicate the two major classes of the company clients, and the stakeholders in the company comprehensively informed the breach and the measures which were taken to ensure that security is tight (Perlroth, 2014). The dissemination of information is important for the public to feel that something is being done towards dealing with security challenges.

5.1.5 Resolution and System Security Enhancements

To resolve the breach and secure their systems, eBay took several steps some of which are as follows:

- **Engaged with External Experts:** Such specialists are hired by an organization whenever an organization wants to get a correct impression of its security posture. This involved doing research and equally identifying the security gaps that exists (Goodin, 2014). Continued communication with the outside environment is useful in getting a third-party security audit which is important in coming up with several security recommendations within an organization. eBay hired experts to review their security policies, made adjustments and gave better security recommendations.
- **Updated Security Policies:** The company changed/modified some of the measures as recommended by the security policies and practices where the breach was realized. This implied the incorporation of higher levels of protection (Symantec, 2014). It is even more important to redesign the circumstances related to the idea of revisiting the trends in security and the traditional security threats with the help of security policies.
- **Enhanced User Awareness:** As a result of the breach, there were sensitization campaigns to the users of eBay informing them time and again of the existence of varieties of fraudsters online, and educating the users on matters regarding the use of strong passwords (Leyden, 2014). This appears to amplify user sensitization which means that in the future there will be a call to employ safer practices – thus deepening the more potent bromide to any future breach.

6. Conclusion and Recommendations

This section discusses the practical implications of the data breach on eBay, as well as recommendations to avoid similar cases. This chapter is aimed at raising the security activities of eBay, enhancing ways of effective communication and compliance with the law on the protection and use of sensitive data, particularly personally identifiable information.

6.1 Lessons Learned

6.1.1 What eBay Did Right

- **Prompt Password Reset:** To sum up, this particular action performed by eBay to delete users' passwords and make them register new and stronger passwords was sufficient to minimize the impact of the cyber attack. This action helped save users from further misuse of their credentials that had been hacked (eBay Inc. 2014). Smooth password changes are a typical response to violations of this kind as the impact could be limited to the utmost extent (Chapple, Stewart, and Gibson, 2018).
- **Engagement with External Experts:** Cybersecurity practitioners being asked to review the company's security weaknesses and bolster its defences led to eBay being viewed as committed to rectifying the mistakes exposed by the breach. Another good point is to pinpoint what it would require of the experts to enhance the execution of remediation techniques (Goodin, 2014). This partnership provided eBay with professional support that had been necessary when enhancing the company's security shields and eradicating insecurity issues.
- **Improved Transparency:** After the breach, eBay began to show greater public relations and started informing the users and the other parties involved. This involved availing information on the data breach incident and other steps being undertaken to strengthen security (Leyden, 2014). Unfortunately, the communication needs to be good to regain the trust, as well as to continuously inform the stakeholders of the other safety factors (Diogenes and Ozkaya, 2018).

6.1.2 What eBay Did Wrong

- **Delayed Response:** This was one of the many grievances that were laid on the doorstep of eBay, particularly regarding the latency to informing the public of the breach. The occurrence was discovered in February 2014, but eBay failed to come out to the public to reveal the same until May 2014. This delay may have exposed those users to identity theft as has been indicated by Perlroth (2014).

- **Inadequate Initial Security Measures:** This report also finds that eBay's poor first-tier security model did not well implement network segmentation and monitoring mechanisms. Among the mentioned shortcomings, the attackers were able to achieve lateral movement within the scope of the organization's network and get access to privileged information (Symantec 2014). Thus, to protect the systems from breaches they need to have a strong security design with numerous levels of security.
- **Lack of Employee Training:** The kind of phishing attack that led to the breach exposed the organization's vulnerabilities in training the employees in matters concerning cybersecurity threats. Perhaps, levels of training and additional promotion of awareness sessions could have assisted in countering some of the aspects of credential theft (Jakobsson & Myers, 2006). The work established that there is a need to supplement the training of the employees on the aspect of social engineering more often and broadly.

6.2 Recommendations for Preventive Measures

6.2.1 Enhanced Security Practices

- **Strengthened Phishing Prevention:** Similarly, eBay should employ today's effective methods of combating phishing and sometimes conduct staff meetings to discuss the issue of phishing scams. This includes an approach that involves forwarding fake phishing emails mainly to an organization's workers as a way of identifying their level of preparedness (MedeAnalytics, 2015). Thus, organizational anti-phishing measures and especially awareness of the company's employees will be the crucial factors to counteract credential theft (Diogenes and Ozkaya, 2018).
- **Improved Network Segmentation:** To minimize the lateral movement of the attackers eBay should enforce network segmentation and access controls to its networks, this way, the network is segmented into sub-sections such that the impact of a breach is contained (Hayden, 2010). Division of parts of work in the network can reduce the enemy's input and avoid problems with leakage in case of a violation.
- **Advanced Monitoring and Detection:** eBay has to implement upper-level antidetection and antiprevention systems to provide a more suitable reaction to possible cyber criminal

activities. Also, constant scanning and immediate notifications of potential incidents will be useful to avoid potential threats (Symantec, 2014, p. 68). Innovatively, threat identification and the early response to threats are very vital in minimizing the impacts of a threat.

6.2.2 User and Stakeholder Communication

- **Timely Notification:** The business should establish measures for informing the users as well as the stakeholders if there is a compromise of their data. Failure in communication exposes the business to risks and leads to a lack of trust (eBay Inc., 2014). The other principle is timely communication for setting the atmosphere of handling the circumstances that result from the violation and the assistance given to those working for the organization.
- **Transparency in Breach Response:** There are some pitfalls which are typical for most firms during the breach investigation and resolution process; one of them is the attempt to conceal information about the breach. eBay also should let users and stakeholders know about the status of breaches from time to time and generate reports through which it would be possible to show commitments to security measures (Leyden, 2014). This period should bring clarity to the operations of the organization

6.2.3 Policy and Regulatory Compliance

- **Adherence to Data Protection Regulations:** Regarding the legal factors, eBay should respect the data protection legal requirements in its business such as GDPR or CCPA. There should be regular audits of the organisation's data protection practices as those recommendations promulgated in the laws and standards of the EU GDPR (European Commission, 2018). This implies that it is not just a legal requirement but an exercise of good responsibility in compliance with security best practices.
- **Implementing Best Practices:** Some of the measures that would assist in the prevention of future equivalent breaches into eBay’s systems and would also assist in safeguarding

the company's data include putting in place data security and privacy measures such as the NIST Cybersecurity Framework (NIST, 2018).

6.3 Summary of Main Findings and Personal Reflections

This 2014 eBay data breach raised many questions concerning the protection of employees' data, lack of negligence regarding adequate security within eBay and other firms, and delay in informing the employees about security breaches. Although eBay had sought to make several commendable manoeuvres such as urging clients to change their passwords and liaising with security experts after the breach, the overall incident handling and the circumstances that led to the breach had vices which needed improvement. The following recommendations should be considered in the future. eBay should come up with better and more enhanced security measures, a better and more efficient way of communicating with and engaging customers and users and also the stakeholders during and after security incidents, and lastly, there should always be consideration for the data protection regulations such as GDPR.

7. References

Bosworth, S., Kabay, M.E. and Whyne, E. (2014) Computer Security Handbook. 6th ed. NJ: John Wiley and Sons, Inc.

Brooks, C.J. et al. (2018) Cyber Security Essentials. John Wiley and Sons, Inc.

Chapple, M., Stewart, J.M. and Gibson, D. (2018) CISSP Certified Information Systems Security Professional: Official Study Guide. 8th ed. Indianapolis, Indiana: John Wiley and Sons, Inc.

Diogenes, Y. and Ozkaya, E. (2018) Cyber Security - Attack and Defense Strategies - Infrastructure with Red Team and Blue Team tactics. Birmingham: Packt Publishing.

eBay Inc. (2014) eBay Inc. to Ask eBay Users to Change Passwords. Available at: https://www.ebayinc.com/stories/news/ebay-inc-ask-ebay-users-change-passwords/ (Accessed: 20 July 2024).

eBay Inc. (2020) About eBay. Available at: https://www.ebayinc.com/company/ (Accessed: 20 July 2024).

European Commission (2018) General Data Protection Regulation (GDPR). Available at: https://ec.europa.eu/info/law/law-topic/data-protection_en (Accessed: 20 July 2024).

Gollmann, D. (2011) Computer Security. 3rd ed. Chichester: Wiley.

Goodin, D. (2014) ‘eBay breach impacted 145 million users, the company now says’, Ars Technica. Available at: https://arstechnica.com/information-technology/2014/05/ebay-breach-impacted-145-million-users-the-company-now-says/ (Accessed: 20 July 2024).

Harris, S. (2018) CISSP All-in-One Exam Guide. 8th ed. McGraw-Hill.

ISO (2022) ISO/IEC 27001:2013 Information security management. International Organization for Standardization.

Jakobsson, M. and Myers, S. (2006) Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft. Hoboken: Wiley.

Kaufman, C., Perlman, R. and Speciner, M. (2002) Network Security: Private Communication in a Public World. 2nd ed. Upper Saddle River: Prentice Hall.

Leyden, J. (2014) ‘eBay finally asks users to change passwords, three months after mega-breach’, The Register. Available at: https://www.theregister.com/2014/05/21/ebay_password_breach/ (Accessed: 20 July 2024).

MedeAnalytics (2015) Privilege Escalation: An In-Depth Analysis. Available at: https://www.medeanalytics.com/insights/privilege-escalation (Accessed: 20 July 2024).

Menezes, A., van Oorschot, P. and Vanstone, S. (1996) Handbook of Applied Cryptography. Boca Raton: CRC Press.

NIST (2018) Framework for Improving Critical Infrastructure Cybersecurity. Available at: https://www.nist.gov/cyberframework (Accessed: 20 July 2024).

Perlroth, N. (2014) ‘eBay discloses massive data breach affecting 145 million users’, The New York Times. Available at: https://nytimes.com (Accessed: 20 July 2024).

Perlroth, N. (2014) ‘eBay’s Security Breach: Corporate Networks Under Siege’, The New York Times. Available at: https://bits.blogs.nytimes.com/2014/05/21/ebays-security-breach-corporate-networks-under-siege/ (Accessed: 20 July 2024).

Pfleeger, C.P. and Pfleeger, S.L. (2012) Security in Computing. 5th ed. Upper Saddle River: Prentice Hall.

SANS Institute (2020) Cybersecurity Trends. Available at: https://sans.org (Accessed: 20 July 2024).

Smith, R. and Rupp, S. (2017) Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions. Hershey: IGI Global.

Stallings, W. (2017) Cryptography and Network Security: Principles and Practice. 7th ed. Upper Saddle River: Prentice Hall.

Symantec (2014) Internet Security Threat Report. Available at: https://www.symantec.com/security-center/threat-report (Accessed: 20 July 2024).

Symantec (2018) Internet Security Threat Report. Available at: https://www.symantec.com/security-center/threat-report (Accessed: 20 July 2024).