**Analysis of Yahoo Breach**

As technology rapidly evolves, virtual businesses must continually evaluate and mitigate the risks of their systems. This is true as cyber-attacks have been trending for the last decade. According to an article by Infosec (Crane), the frequency of cyber-attack incidents with reported losses of over $1 million increased from 21 to 105 cases between 2009 and 2019. For business, the maturity of the fact tends to be ignored as long as their business is operational. Thus, attacks at businesses that belong to the described description are susceptible to massive data breaches and irreparable damage to their brand. Yahoo exemplifies this case with its 2013-2014 breach, it is discovered in 2016 and resolved a year after that. Note that the breach being referred to is the breach against Yahoo’s internal network, not the breach against individual Yahoo user accounts. Although these breaches are connected, the paper will mainly focus on the breach in Yahoo’s internal network to narrow the scope of analysis. This paper aims to use Yahoo to examine the complexity of threats, vulnerabilities, and needed controls to address the vulnerabilities exploited. The paper will also examine how Yahoo, as a leading mail organization, handled the breach and the comparison of their implemented control to the control generated from the vulnerability exploited. Before analyzing the breach, general context of the company and breach must be established to understand the magnitude of the breach.

**The Company**

Yahoo is a web service headquartered in Sunnyvale, California. Founded in 1995, Yahoo was the leading example of media and email services during the early days of the internet. Since they provide various services internationally, their competitors include multinational companies such as Microsoft, Google, AOL, and Baidu (Comparably). To compete with these large companies, Yahoo must continue to create innovative services using advanced technologies, such as cloud storage. It is imperative for any business to mitigate and address the inherent risks of adopting new technologies. Yahoo’s stance on this issue lacks maturity as it provided minimal investment to the issue. This is proven by the frustration of Alex Stamos, Yahoo’s CISO (Chief Information Security Officer), who declared having received insufficient funding to secure Yahoo systems from Marissa Mayer, Yahoo’s CEO (Perlroth). With little investment in their security, Yahoo’s efforts to remain on top of their competitors were put to a pause due to significant breaches of their system and user data.

**The Breach**

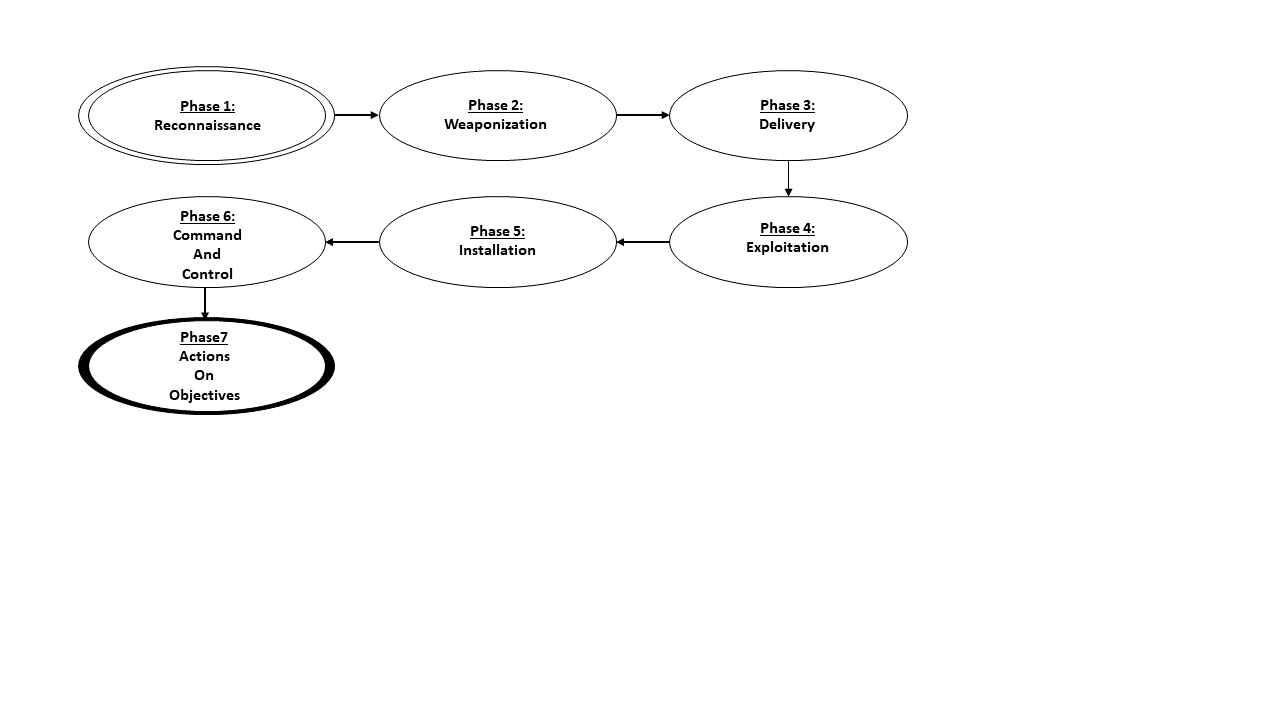
In 2016, Yahoo discovered their user data was being sold on an underground website. The data being sold was advertised to include 200 million yahoo accounts that revealed the following information: Yahoo login (ID), Country Code, Recovery E-mail, Date of Birth, Hash of Password, Cellphone, and Zipcode (Plesco). Yahoo acknowledged this breach and asked users to change their password as a response. However, Yahoo did not publicly announce the breach to the public since the legitimacy of the data dump was not verified. 18 months later, Yahoo publicly acknowledged the breach and claimed that 500 million Yahoo accounts were compromised.

Yahoo’s public acknowledgment revealed that the breach occurred in 2014 and was conducted by state-sponsored attackers. Due to the origin of the attack, the FBI became another key figure investigating the breach. Their role in the investigation is to apprehend the attackers by focusing on the origin of the discovered data dump. Another key figure in this investigation is Andrew Komarov, the chief intelligence officer of InfoArmor, as his actions revealed another breach that occurred in 2013 by the same attackers. While Yahoo focused on recovering their security and overall image, Komarov further investigated the origins of the data dump. His investigation discovered another set of data dump containing 1 billion user accounts, which also consist of accounts that are directly correlated to the US government, US military, European Union, Canadian governments, British governments, and Australian governments (May). Further investigations have increased the number of compromised to 3 billion users, accounts, which is equivalent to every Yahoo user in 2013. In essence, Yahoo suffered from a large breach, occurring from 2013 to 2014, which was reported in 2016. Fortunately for Yahoo, the attackers were apprehended in 2017 and brought to trial in the US on February 28th of the same year. Following the documented testimonies in the court reveals all the threats used to breach Yahoo.

**The Threats**

Much Academic analysis of Yahoo’s breach has described it as a case study to use the cyber kill chain model to understand the threats deployed by the attackers. Derived from the military concept of kill chain, cyber kill chain is a process of defining an attack from a source (Spitzner). Figure 1 defines the model to include the following phases: Reconnaissance, Weaponization, Delivery, Exploitation, Command and Control, and Actions on Objectives. The source of the attack is a black hat hacker, which is a type of threat that describes criminals that intrude system networks with malicious intent. As detailed within court documents, the black hats are discovered to be state-sponsored attackers originating from Russia (UNITED). Their intention of breaching Yahoo’s system is to access employees of the following commercial entities: a French transportation company, U.S. financial services and airlines, and Swiss bitcoin wallets and banking firms. As black hat hackers, they deployed numerous threats to breach Yahoo’s internal network. By using the cyber kill chain as a framework, an in-depth analysis can be made in describing malicious activities and types of threats deployed to the Yahoo network by the black hat hackers.

Figure 1: Cyber Kill Chain Framework



Phase 1: Reconnaissance

The type of threat that exists within the reconnaissance phase is the name of the phase itself. Reconnaissance is known as a threat used to identify systems, assets, and their respective configurations for malicious purposes (Richardson). The attackers used this threat to identify emails of staff members, which are the assets, along with any associated recovery email. Assisted by their respective government, the attackers identified emails of staff members that acquire semi-privilege and not top executives. With a targeted group, the next phase is weaponization, which prepares the logistics of delivering a payload to the targeted user.

Phase 2: Weaponization

The types of threats within the weaponization phase are threats that build a type of deliverable that can lead to an exploit and backdoor. Since this phase acts as a preparation for the next phase, no threats were used. However, the activity within this phase is important to note as it creates a layer of complexity on the deployment of threats. The layer of complexity is defined as the action of leasing servers in Arizona and Illinois (Abdollah). Their goal of this action is to disguise their digital footprint, such that any digital forensic analysis would find that they originate within the U.S rather than Russia. The action also serves another goal of using their virtual geographic location to create authentic emails, which is heavily relied on in the next phase. With deliverability determined, the next phase is delivery, which delivers a payload using the described method of delivery.

Phase 3: Delivery

The type of threats within the delivery phase are threats that send a payload using the deliverable created in the previous phase. The threats present within this phase are spearfishing, a type of social engineering threat, by using emails generated under a VPN. Spearfishing is a targeted attack to steal information by appearing as an authentic and legitimate user requesting personal information (Kaspersky). The attackers used spearfishing by sending emails to Yahoo staff with semi privilege along with their associated recovery email. These emails are sent using the email accounts created from the previous phase. Since the emails are authentically generated from various locations, this layer of complexity increases the chances of the user perceiving emails as authentic rather than deceptive. With the malicious email sent, the next phase, exploitation, describes the underlying threat attached to the email.

Phase 4: Exploitation

The type of threats within the exploitation phase include threats that execute code from the payload described in the previous phase. In this case, the code executed is whatever the user interacts with within the email. According to Ryan Nye’s analysis of the spearfishing Yahoo endured, attached to the email is a link that prompts the target to reset their user to a dummy site (Nye). Since the dummy site is hosted by the attackers, the target's inputted credentials will be saved in the server for the attackers to use. This guarantees attackers an unauthorized passage to Yahoo's network. Note that this activity is an extension of spearfishing, thus not a new threat. With access to Yahoo’s internal network, the next phase, installation, describes installing software in Yahoo’s system.

Phase 5: Installation

The type of threats within the installation phase includes threats that include software designed to damage or gain unauthorized access to the system. The threat present within this phase is malware that collects user information within Yahoo’s user database. Once enough information is obtained, the malware generates cookies for a specified user, providing unauthorized access to all Yahoo users (U.S). Since the Yahoo user database also includes staff members, attackers also gain another backdoor into Yahoo’s network through forged cookies generated by the malware. The attackers also implemented a log cleaner within Yahoo’s system. Since log cleaners are not inherently malicious, they are not a threat. However, they benefit attackers as the log cleaner will erase any digital footprint they left within Yahoo’s system. With malicious programs installed within the system, the next phase command-and-control describes how the attackers maintain access to Yahoo’s assets.

Phase 6: Command and Control

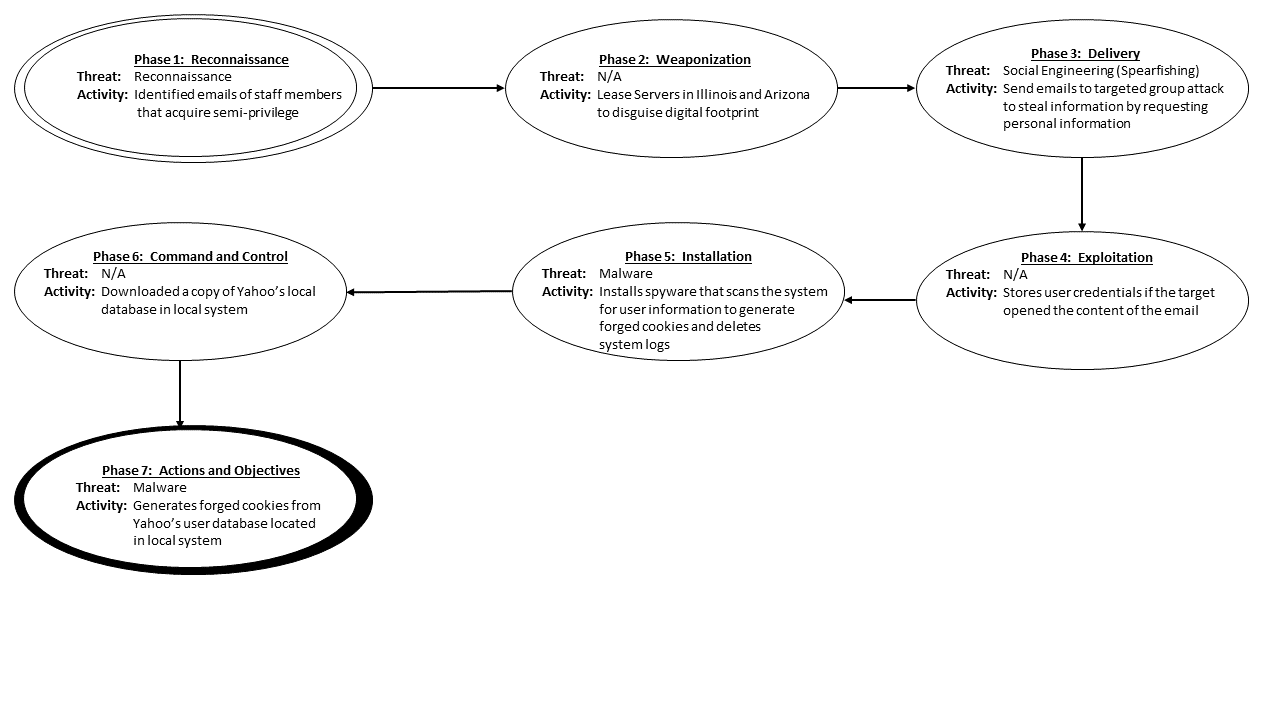
The type of threats within the command-and-control phase includes threats that remotely controls the targeted system and its assets. Unfortunately, this topic was not covered comprehensively during the attackers’ indictment. The attackers’ activities during this phase are described as utilizing FTP (File Transfer Protocol) software to transfer a copy of Yahoo’s user database to their local computer (Ohlhorst). This guarantees the attackers a secure way of accessing Yahoo’s user database in a way that Yahoo cannot prevent. Since using FTP is not malicious, this activity is not a threat. However, it provided the attackers more ways to damage Yahoo’s system without being present in Yahoo’s internal network. With on-demand and secure access to Yahoo’s user database, the attackers continue to the last phase, actions and objectives, which are activities that carry out the attackers’ goal.

Phase 7: Actions and Objectives

The type of threats within the actions and objectives phase includes threats that carry out their goal. The threat used within this phase is malware, which generates forged cookies using a copy of Yahoo’s database in the attackers’ local system (Gallagher). As a result, the attackers can generate forged cookies outside of Yahoo’s system without leaving any digital footprint within Yahoo’s system. Since the malware is not installed within Yahoo system, this limits Yahoo’s actions against the attackers’ capability to generate forged cookies to access their system.

In summary, black hat hackers were the main threat of Yahoo's breach. As black hat hackers, their goal was to access commercial entities through individuals with semi-privileges. Using the cyber kill chain framework, the black hat hackers achieved their goal by deploying the following threat: reconnaissance, social engineering through the means of spearfishing, and malware. A succinct description can be viewed in Figure 2, where phases of the cyber kill chain process are associated with their respective actions and threats. With threats analyzed, further exploration of Yahoo's breach can be viewed from an analysis of Yahoo's vulnerabilities that enabled the previously listed threats from occurring.

Figure 2: Activities and Threats in Relation to Cyber Kill Chain Framework



**The Vulnerabilities**

To react effectively against Yahoo’s breach, vulnerabilities exploited by the threats analyzed must be identified. By recalling and activities and threats that occurred during the breach, Yahoo’s attackers exploited vulnerabilities in the following area: authorization, access, system hardening, nonrepudiation, and information disclosure.

Authorization

Authorization is the assurance that the system can identify a user within a system, such that the system can restrict or allow access to the system and its assets. The attackers exploited a vulnerability in authorization by using Yahoo staff credentials to access Yahoo’s internal network through means of social engineering (Kovach). This allows the attackers to access Yahoo’s internal system by using stolen authentic credentials. Since the attackers is now disguised as an authorized user, the system can no longer prevent and restrict the attackers from accessing Yahoo’s internal system and its assets. This exploitation may evolve to greater harm since Yahoo failed to implement comprehensive access controls.

Access

Access is the accommodation of needed capabilities to an individual in the system. The attackers exploited a vulnerability in access by using the same set of compromised credentials to both access the external and internal system of Yahoo’s system (pindrop). Essentially, this allows the attackers to access the entire Yahoo system by only using one compromised credential. Recalling the attackers’ target of semi-privileged users, Yahoo clearly made an error in providing semi-privileged users access to the entire system, which provided a gateway to Yahoo’s entire user database. Another error that is worth mentioning is allowing semi-privileged users to download software’s within Yahoo’s internal system. In essence, if these vulnerabilities were addressed, the magnitude of the breach would not be as damaging as it was. The vulnerability can also be perceived as a system hardening capability.

System Hardening

System hardening is the guarantee that the system only performs the desired functions. The attackers exploited a vulnerability in system hardening by downloading multiple software within Yahoo’s internal system and transferring large files, such as a copy of Yahoo’s user database, to external systems through FTP without warning or alerts. With no restrictions in inbound and outbound activities, these vulnerabilities portray the attackers as having no restrictions on their activities, which is equivalent to being a root user. If Yahoo had implemented more logical firewall rules, much of what the attackers’ achieved would not be possible. Since this exploit is enabled by a lack of warning or alerts, this can also be perceived as a vulnerability in nonrepudiation.

Nonrepudiation

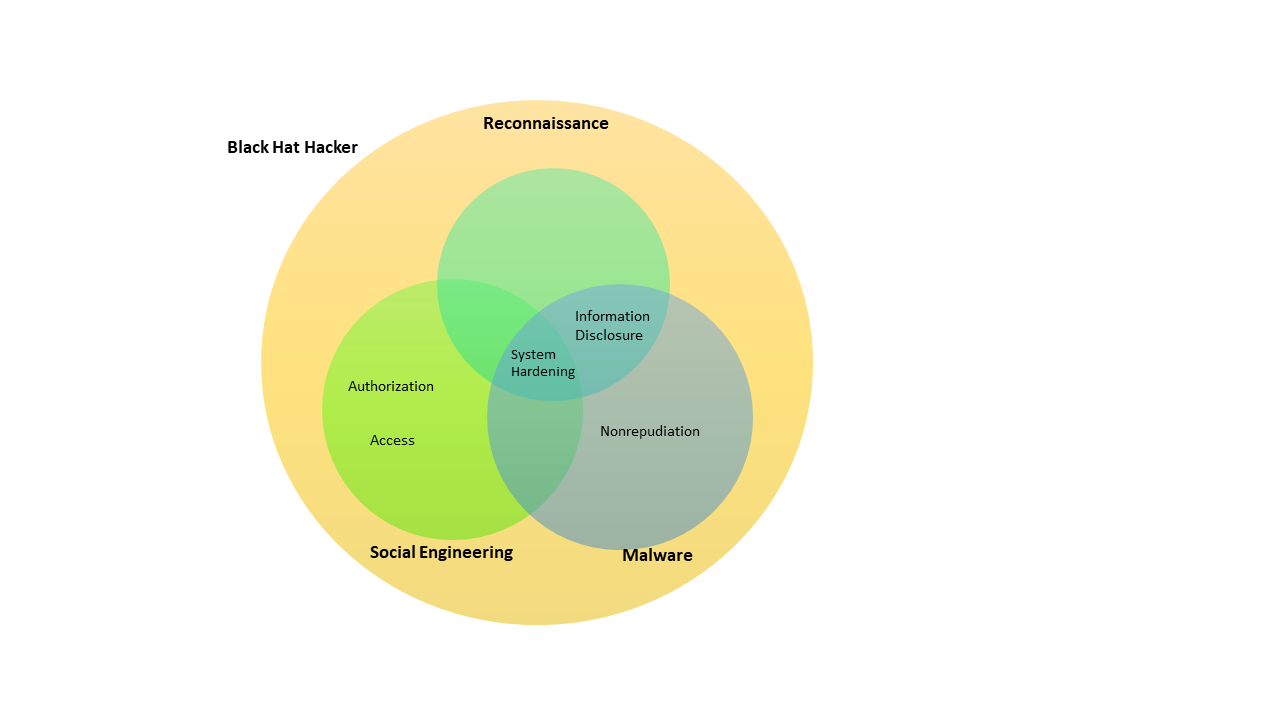
Nonrepudiation is the ability to prove the activities within a system. The hackers exploited a vulnerability in nonrepudiation by Yahoo’s lack of alerts on their internal system. With the lack of alerts, the attackers managed to transfer a copy of their user database and download a log cleaner software within their system. As a result, the attackers left minimal digital footprint, leaving Yahoo with little information on when and how their system was compromised along with their associated activities. This lack of information on Yahoo’s part is expressed during early investigations as they claimed that the breach only occurred once when it occurs twice. To prove this point further, their claim was later disproven because the investigation found more user data being sold originating from another breach rather than any data from logs.

Information Disclosure

Information disclosure is generally understood as the presentation of information for system functionality. However, the definition can be extended further to include protecting sensitive and confidential information from unauthorized parties (netsparker). With this definition in mind, the attackers exploited a vulnerability in information disclosure by reading encrypted and unencrypted data in Yahoo’s user database. In addition to storing data without encryption, Yahoo encrypted some of its data using the MD5 algorithm, which, by 2009, is a widely recognized weak and deprecated algorithm. Thus, Yahoo’s persistence to continually use the algorithm resulted in providing the attackers user information to create authentic cookies using software that generates forged cookies. This issue could also be viewed as a vulnerability in system hardening and nonrepudiation as Yahoo’s use of weak and deprecated code provided the attackers passive reconnaissance of all Yahoo users, which ultimately lead to another breach in the same year.

In summary, Yahoo’s vulnerability in authorization, access, system hardening, nonrepudiation, and information disclosure enabled the attackers to access Yahoo’s internal network, leave a backdoor for later access, and copy their user database to a local machine. Figure 3 portrays this relationship succinctly by associating a vulnerability exploited to the main threats of the breach. With threats and vulnerabilities analyzed, the appropriate sets of control objectives that address the breach can be generated.

Figure 3: Threats and the Vulnerabilities Exploited



**Control Objectives**

With the threats and vulnerabilities analyzed, control objectives can be generated to patch the described exploits in the future. Control objectives are objectives that describe the type of controls that can be implemented to address a set of threats and vulnerabilities. Once controls are implemented, control objectives can be further used as a metric by comparing the outcome of the control to the overall objective of the control. Table 1 describes the control objectives that are generated according to the vulnerabilities and threats described in their respective sections. Note that the structure of Table 1 is heavily influenced by Dr. Lidster’s analysis of Target’s Breach.

Table 1: Generated Control Objectives with Respect to Threats and Vulnerabilities

|  |  |  |
| --- | --- | --- |
| **Threat** | **Vulnerability Category** | **Control Objectives** |
| Black Hat Hacker | Authorization | Reduce the likelihood of authorizing compromised credentials |
| Access | Validate users for high privilege operations, such as downloading software in internal systems |
| System Hardening | Limit user activity according to their privilege, such that semi-privileged users cannot download and execute third party software |
| Nonrepudiation | Alert any inbound traffic from unrecognizes systems |
| Information Disclosure | Protect all data from being viewed from under privileged users. |
| Reconnaissance | Information Disclosure | Prevent passive reconnaissance on unencrypted and encrypted data in databases |
| System Hardening | Secure all user data via encryption |
| Social Engineering | Access | Diversify credentials used to access internal and external Yahoo systems |
| Authorization | Reduce the likelihood of authorizing compromised credentials |
| System Hardening | Limit activities within the system for semi-privilege users |
| Malware | System Hardening | Disable software and its associated activities that are not recognized within the system. |
| Nonrepudiation | Alert any outbound traffic to unrecognized systems. |
| Information Disclosure | Secure data encryption by using approved and updated encryption algorithms. |

Although the table above provides comprehensive control objectives that address the threats and vulnerabilities discussed, Yahoo’s own generated control objectives in response to the breach are narrow in comparison.

**Yahoo’s Response**

A summary of Yahoo’s response to the breach can be examined through four key actions. The first key action is invalidating unencrypted security questions and answers (Lord) and forged cookies. This prevents attackers from accessing the Yahoo user account without a password or using security questions and answers to create a new password with a recovery email. This action also removes any backdoors towards Yahoo's system that uses forged cookies.

The second key action is enhancing the system to detect and prevent unauthorized access (Matthews). This action solves the lack of alerts for unauthorized access within Yahoo’s system. As a result, this reduces the likelihood of a successful attempt at social engineering, such as spearfishing.

The third key action is prompting all users to change their passwords (Goel). This action invalidates all the data stolen from the copy of the database the attackers downloaded to their local computer. This action also invalidated all forged cookies created externally from the stolen copy of the database since forged cookies are generated using a set of information. Once information is modified, a different cookie must be generated according to the modified set of information.

The last key action is creating smart warnings and alerts (Yahoo). Yahoo defines this new feature by detecting malicious content in e-mails. This reduces the chance of any successful social engineering for Yahoo employees in the future by alerting employees of a potentially malicious email.

In terms of comparison, Table 2 describes Yahoo’s key actions in response to the breach against the control objectives generated to address threats and vulnerabilities of the breach. Note that the structure of Table 2 is heavily influenced by Dr. Lidster’s analysis of Target’s Breach.

Table 2: Generated Control Objectives with Respect to Threats and Vulnerabilities

|  |  |  |  |
| --- | --- | --- | --- |
| **Threat** | **Vulnerability Category** | **Control Objectives** | **Yahoo’s Actions** |
| Black Hat Hacker | Authorization | Reduce the likelihood of authorizing compromised credentials | Invalidate forged cookies and unencrypted user’s questions and answers |
| Access | Validate users for high privilege operations, such as downloading software in internal systems | Enhance system to detect and prevent unauthorized access |
| System Hardening | Limit user activity according to their privilege, such that semi-privileged users cannot download and execute third party software | N/A |
| Nonrepudiation | Alert any inbound traffic from unrecognizes systems | N/A |
| Information Disclosure | Protect all data from being viewed from under privileged users. | Enhance system to detect and prevent unauthorized access |
| Reconnaissance | Information Disclosure | Prevent passive reconnaissance on unencrypted and encrypted data in databases | Invalidate unencrypted security questions and answers |
| System Hardening | Secure all user data via encryption | Invalidate unencrypted security questions and answers |
| Social Engineering | Access | Diversify credentials used to access internal and external Yahoo systems | N/A |
| Authorization | Reduce the likelihood of authorizing compromised credentials | Creating smart warnings and alerts |
| System Hardening | Limit activities within the system for semi-privilege users | Enhance system to detect and prevent unauthorized access |
| Malware | System Hardening | Disable software and its associated activities that are not recognized within the system. | N/A |
| Nonrepudiation | Alert any outbound traffic to unrecognized systems. | N/A |
| Information Disclosure | Secure data encryption by using approved and updated encryption algorithms. | N/A |

The comparison between Yahoo’s action and the generated control objectives reveals that much of Yahoo’s actions are directed to enhance security in terms of access and encryption. Although both are improvements to the system, there are still apparent issues with Yahoo’s management of malicious activity within the system. With the current actions, the system is still susceptible to breaches, especially with threats such as Insiders. Insiders are authorized users, such as a member of the company, who engage in malicious activities in their company’s system. Since their activities originate from authorized access, Yahoo’s system cannot prevent their actions. Thus, Yahoo’s system will suffer from this threat as they still do not have any controls on detecting, alerting, and disabling activities.

**Summary**

Between 2013-2014, Yahoo suffered a breach that compromised 3 billion users, which is equivalent to all Yahoo users in 2013. The breach was a result of a black hat hacker, whose goal is to access employees of international commercial entities. Using the cyber kill model, the identified threats deployed by the black hat hacker consists of reconnaissance, social engineering, and malware. An analysis of the threats revealed that Yahoo suffered from vulnerabilities in access, authorization, system hardening, nonrepudiation, and information disclosure. Using this information, control objectives are generated to address each vulnerability. In comparison, Yahoo’s key actions as a response to the breach only consist of preventing unauthorized access, encryption of data, and identifying malicious emails. With a lack of actions in detecting malicious activities within their internal system, Yahoo is still susceptible to threats such as an Insider, where an authorized individual of Yahoo can engage in malicious activities within the system without prevention or any alert to Yahoo. Although Yahoo evolved their cybersecurity capabilities, it comes at the cost of compromising every single Yahoo user in 2013. As a result, Yahoo’s breach has shrunken its reputation as one of the leading email services to a case study in the lack of security maturity for web services.

**Resources**

Abdollah, Tami. “Prosecutors: Russian Hackers Exploit US Cyber Vulnerability.” *AP NEWS*, Associated Press, 17 July 2018, apnews.com/article/02c6ac7e3f51433cbfd04530c0108e37.

Comparably. “Yahoo Competitors.” *Comparably*, Comparably, 11 Mar. 2020, www.comparably.com/companies/yahoo/competitors.

Crane, Casey. “42 Cyber Attack Statistics by Year: A Look at the Last Decade.” *InfoSec Insights*, Sectigo Store, 6 Nov. 2020, sectigostore.com/blog/42-cyber-attack-statistics-by-year-a-look-at-the-last-decade/.

Gallagher , Sean, and Dan Goodin. “US Charges Two Russian Agents with Ordering Hack of 500m Yahoo Accounts.” *Ars Technica*, WIRED Media Group, 15 Mar. 2017, arstechnica.com/tech-policy/2017/03/us-charges-two-fsb-officers-two-criminal-hackers-in-yahoo-breach/?comments=1.

Goel, Vindu, and Nicole Perlroth. “Yahoo Says 1b of Its User Accounts Were Hacked Into.” *Australian Financial Review*, Australian Financial Review, 15 Dec. 2016, www.afr.com/technology/yahoo-says-1b-of-its-user-accounts-were-hacked-into-20161215-gtbhiv.

Kaspersky. “What Is Spear Phishing? - Definition.” *Usa.kaspersky.com*, Kaspersky, 11 Feb. 2019, usa.kaspersky.com/resource-center/definitions/spear-phishing.

Kovach, Steve. “FBI: Russian Hackers Likely Used a Simple Phishing Email on a Yahoo Employee to Hack 500 Million User Accounts.” *Business Insider*, INSIDER, 16 Mar. 2017, www.businessinsider.com/fbi-yahoo-hackers-used-spear-phishing-email-gain-access-500-million-accounts-2017-3.

Lord, Bob. “Important Security Information for Yahoo Users.” *Yahoo*, Yahoo, 15 Dec. 2016, yahoo.tumblr.com/post/154479236569/important-security-information-for-yahoo-users.

Matthews, Kayla. “Incident Of The Week: Multiple Yahoo Data Breaches Across 4 Years Result in a $117.5 Million Settlement.” *Cyber Security Hub*, Cyber Security Hub, 7 Oct. 2019, www.cshub.com/attacks/articles/incident-of-the-week-multiple-yahoo-data-breaches-across-4-years-result-in-a-1175-million-settlement.

May, Patrick. “How a Super Cyber-Sleuth Helped Crack the Huge Yahoo Hack.” *The Mercury News*, The Mercury News, 16 Dec. 2016, www.mercurynews.com/2016/12/15/how-a-super-cyber-sleuth-helped-crack-the-latest-yahoo-hack/.

Netsparker, Security Team. “Information Disclosure Issues and Attacks in Web Applications.” *Netsparker*, Netsparker, 19 June 2019, www.netsparker.com/blog/web-security/information-disclosure-issues-attacks/.

Nye, Ryan. “A ‘KILL CHAIN’ ANALYSIS OF THE 2016 YAHOO! DATA BREACH.” *Rnyte-Cyber*, UNIVERSITY OF SAN DIEGO, 14 Aug. 2017, www.rnyte-cyber.com/uploads/9/8/5/9/98595764/ckcyahoo\_by\_rnye.pdf.

Ohlhorst, Frank. “FTP Remains a Security Breach in the Making.” *TechRepublic*, TechRepublic, 30 July 2014, [www.techrepublic.com/article/ftp-remains-a-security-breach-in-the-making/](http://www.techrepublic.com/article/ftp-remains-a-security-breach-in-the-making/).

Perlroth, Nicole, and Vindu Goel. “Defending Against Hackers Took a Back Seat at Yahoo, Insiders Say.” *The New York Times*, The New York Times, 28 Sept. 2016, www.nytimes.com/2016/09/29/technology/yahoo-data-breach-hacking.html?\_r=0.

Pindrop. “500 Million Users Affected by Yahoo Data Breach.” *Pindrop*, 8 Sept. 2017, www.pindrop.com/blog/500-million-users-affected-by-yahoo-data-breach/.

Plesco, Todd. “Yahoo's Exfiltration of MD5 Credentials.” *INFORMATION SECURITY PRO*, INFORMATION SECURITY PRO, 29 Sept. 2016, www.infosecurity.pro/?p=7252.

Richardson, Stephen. “Threat Reconnaissance Attacks - Network Design.” *Cisco Certified Expert*, Cisco Certified Expert, 6 Sept. 2020, www.ccexpert.us/network-design/threat-reconnaissance-attacks.html.

Spitzner, Lance. “Applying Security Awareness to the Cyber Kill Chain.” *Information Security Training*, SANS, 28 Feb. 2020, www.sans.org/security-awareness-training/blog/applying-security-awareness-cyber-kill-chain.

“U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts.” *The United States Department of Justice*, 21 Mar. 2017, www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions.

“UNITED STATES OF AMERICA VS DMITRY DOKUCHAEV, a/k/a ‘Patrick Nagel," IGOR SUSHCHIN, ALEXSEY BELAN, a/k/a ‘Magg," and KARIM ·Vc SARATOV, a/k/a ‘Kay," a/k/a ‘Karim Taloverov," a/k/a ‘Karim Akehmet Tokbergenov.’” *Https://Www.justice.gov/*, U.S. Department of Justice, 28 Feb. 2017, www.justice.gov/opa/press-release/file/948201/download.

Yahoo. “Additional Security Features in Yahoo Mail | Account Help - SLN29297.” *Yahoo!*, Yahoo!, help.yahoo.com/kb/account/additional-security-features-yahoo-mail-sln29297.html.