Corporate Profile Part 2: Cybersecurity Risk Profile

Yahoo! Inc.

DeBora King

CSIA 350 6380

Cybersecurity in Business and Industry (2172)

February 4, 2017

EXECUTIVE SUMMARY

Business Profile

What began as a hobby for two Stanford University students 23 years ago, Yahoo! has become one of the world's largest global search engine services. In 1994, Yahoo! co-founders, David Filo and Jerry Lang, set out to find and effective and efficient way to surf the world-wide web by designing a search engine Their tool grew from a group full of happy friends up to a million users a day by 1998 (Entrepreneur). In 2015, Yahoo's search engine services generated 42% of their revenue (Hoovers). In addition to search engine services, which is shared with Microsoft's Bing, Yahoo's communication services include Yahoo mail and messenger services, which are based on a fee if users choose premium service. Services also include digital content products and services: Tumblr, Yahoo News, Yahoo Sports, Yahoo Finance, and Yahoo Lifestyle). Yahoo's advertising services include Gemini and BrightRoll products. Yahoo's global operations draws 22% of its revenue mostly from Asian assets (Yahoo! 2015 Annual Report). Today, Verizon is in the process of buying Yahoo's Internet business for approximately $4.8 billion. An incident that occurred with 500 million Yahoo user accounts being compromised by a hacker didn't help Yahoo's image.

Company Overview

Yahoo! Inc (YHOO on the NASDAQ Global Market) is headquartered in Sunnyvale, California USA. Its key personnel include Eric Brandt, Chairman; Marissa Mayer, President and CEO; Kenneth Goldman, CFO; co-founder, David Filo; and CIO, Laurence Mann (Hoovers). Yahoo's main competitors are Google, AOL, and MSN. Google's competitive edge over Yahoo! is huge having gained almost 65% of the search market in America. Facebook and Twitter's

rising communication services are also competition for Yahoo!. Hoovers reports Yahoo's 2015 annual revenue at $4,968 billion.

Risk Response

Security Controls Identified

The NIST control family can be categorized into three sections: Management, Operational and Technical (Dulaney, 2014). Yahoo's most recent 10-K filing (Annual Report to Investors) identifies their risk factors which can be categorized as follows:

- **Management** – Yahoo's sole existence is dependent on users having access to the Internet. This requires collaboration from Internet Service Providers and telephone companies. Strategic planning is key to Yahoo's business success – without it, all stakeholders will be adversely affected.
- **Operational** – Yahoo's objective is to be accessible, reliable, and dependable in providing products and services without business interruption. Procedures that include system security implementation, maintenance, and continuity is key to operational controls.
- **Technical** – Yahoo's recent security breaches may have damaged user's confidence in the company. In order to regain that confidence, Yahoo must incorporate technical measures to protect consumer personal data.

Possible Products & Services to Include

Since Yahoo is a cloud based business, focusing on solutions that specifically affect their ability to succeed is beneficial to the company. When it comes to cloud computing, security risks are specialized and must be addressed accordingly. Cloud Standards Customer Council provides

10 steps for successful cloud computing (Cloud Standards Customer Council, 2015). These 10 steps include:

1. ensuring effective governance, risk and compliance processes exist,
2. auditing operation and business processes,
3. managing people, roles and identities,
4. ensuring proper protection of data information,
5. enforcing privacy policies,
6. assessing the security provisions for cloud applications,
7. ensuring cloud networks and connections are secure,
8. evaluating security controls on physical infrastructure and facilities,
9. managing security terms in the cloud service agreement, and
10. understand the security requirements of the exit process.

Security Event and Incident Management (SEIM) products can be one of the most effective tools to largely address risk mitigations for Yahoo's objectives. Security Content Automation Protocol (SCAP) scanners, Network traffic capture and monitoring sensors, anti-malware whitelisting, and file integrity assessment tools are also beneficial considerations to mitigate risks. SANS Institute's four main philosophies for implementing controls is 1) tackling the most common and damaging issues, 2) providing consistent controls to guard against attacks, 3) automating defenses, and 4) providing consistent defense for attacks that occur often (SANS, 2011).

Risk Register & Risk Mitigation Approach with Recommended Security Controls

The following chart identifies Yahoo's risks along with their description and risk management strategy. It also lists the risk mitigation approach with recommended security controls from the SP800-53 family identified by NIST (NIST Special Publication 800-53, 2013).

Risk Identifier	Description of the Risk & Current Risk Management Strategy	Risk Mitigation Approach with Recommended Security Controls (by NIST SP 800-53 family)
#1	Complying with unsettled regulatory changes from federal, state, foreign entities in the privacy and protection of user data – the collection, use, retention, disclosure, sharing and security of data stemmed from users.	Audit & Accountability
#2	Avoiding loss of user confidence due to security breach for personal data. Address concerns from users about privacy and protection of user data.	Identification & Authentication
#3	Guard against business interruption due to outages (resulting from fire, flood, earthquake, tsunami or other natural disasters).	Physical & Environmental Protection
#4	Avoiding system malfunctions from human errors after administering design network modifications which could result in services being taken offline for corrective action.	Configuration Management
#5	Address server vulnerability to computer viruses, malware, worms, hacking, physical and electronic break-ins, router disruption, sabotage or espionage, and other disruptions from unauthorized access and tampering, as well as coordinated denial-of-service attacks.	Incident Response
#6	Strengthen controls between third-party providers to prevent failure to deliver products and services.	Contingency Planning
#7	Partner with Internet Service Providers and phone companies to insure users have continued and unimpeded access to the internet which is imperative to the business.	Planning

References

Entrepreneur. n.d. *David Filo & Jerry Yang: The chief yahoos*. Entrepreneur Growth Strategies. Retrieved from https://www.entrepreneur.com/article/197564

Hoovers. Yahoo! Inc. Operations. Retrieved from http://subscriber.hoovers.com.ezproxy.umuc.edu/H/company360/overview.html?companyId=48043000000000

Yahoo! Inc. 2015 Annual Report. Retrieved from https://s.yimg.com/ge/about/yahoo_ar15_annual_report.pdf

Dulaney, E. (2014, July 14). Picture this: A visual guide to security controls. Certification Magazine. Retrieved from http://certmag.com/picture-this-visual-guide-security-controls/

Cloud Standards Customer Council. (2015). *Security for cloud computing ten steps to ensure success 2.0*. Retrieved from http://www.cloud-council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf

Tarala, J. (2011, April). *Implementing the 20 critical controls with security information and event management (SEIM) systems*. SANS Institute. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/implementing-20-critical-controls-security-information-event-management-siem-systems-34965

NIST Special Publication 800-53 Revision 4. (2013, April). *Security and privacy control for federal information systems and organizations*. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf