INDIVIDUAL ASSIGNMENT

NAME (TP NUMBER)	:	Koo Wai Kit (TP081761)
INTAKE CODE	:	APUMF2406CYS
MODULE TITLE	:	Information Security Design (072024-JLL)
MODULE LECTURER	:	Assoc. Prof. Dr. Jalil bin Md Desa
PROJECT TITLE	:	CT108-3-6-M-ISD Individual Assignment
DATE ASSIGNED	:	18/7/2024
DATE COMPLETED	:	29/9/2024

Table of Contents

List of Tables

List of Figures

1.0 Introduction

In today's digital landscape, robust information security design is essential for safeguarding organisational assets and ensuring the protection of sensitive data. Yahoo, once a leading global internet services provider, has faced significant challenges over the years due to security breaches and vulnerabilities. These incidents have not only compromised the personal information of billions of users but also highlighted weaknesses in Yahoo's information security framework. As cyber threats continue to evolve, it becomes critical to reassess and improve the organisation's security posture.

This research aims to examine Yahoo's current information security design, identify key vulnerabilities and risks, and propose targeted improvements to address these weaknesses. By analysing past incidents and evaluating the effectiveness of Yahoo's existing security measures, the research will offer solutions that incorporate the latest security technologies and practices, ensuring the organisation is better equipped to manage emerging threats.

2.0 Yahoo Overview

This section presents an overview of Yahoo, including its company profile, business nature, and organisational structure. It aims to encapsulate Yahoo's role in the technology sector and its evolution in providing a wide range of online services.

2.1 Company Profile

Figure 1: Yahoo Headquarter in Sunnyvale, California (Tikkanen, 2017)

Yahoo! Inc. is a global internet services provider headquartered in Sunnyvale, California (Tikkanen, 2017). Founded in 1994 by Jerry Yang and David Filo, two graduate students at Stanford University, the company initially began as a simple directory of their favourite websites. Originally named "Jerry and David's Guide to the World Wide Web," it was later rebranded as Yahoo!, an acronym for "Yet Another Hierarchical Officious Oracle." Yahoo quickly expanded to offer a variety of services, including a search engine, e-mail service

(Yahoo! Mail), and online gaming (Yahoo! Games), cementing its position as a major player during the dot-com boom of the late 1990s. Tikkanen (2017) mentions that over the years, Yahoo acquired several companies to strengthen its services, including Rocketmail (which became Yahoo! Mail) and the photo-sharing platform Flickr. Despite these efforts, Yahoo struggled to compete with other tech giants, particularly Google.

In 2017, Verizon Communications acquired Yahoo's core assets, including its internet operations, for approximately $4.48 billion (Tikkanen, 2017). The acquisition excluded Yahoo's stakes in Alibaba and Yahoo Japan, leading to a fragmented management structure (Eckstein, 2022). After the acquisition, Yahoo became part of Verizon's subsidiary, Oath, while some parts of the company that was not sold, such as its stake in Alibaba, were reformed into a new entity called Altaba (Tikkanen, 2017). Yahoo continues to operate as a distinct brand under Verizon's ownership, providing a range of online utilities and services.

In September 2021, Apollo Global Management, a prominent private equity firm, acquired 90% of Yahoo and AOL from Verizon for $5 billion (Fischer, 2023; Apollo Global Management, 2021). Following the acquisition, Apollo rebranded the combined entity as Yahoo! and appointed Jim Lanzone as the CEO to lead the business (Fischer, 2023). The acquisition aimed to capitalise on the substantial data resources and ad technology capabilities of both Yahoo and AOL to create a competitive digital advertising platform. However, despite efforts to unify their advertising tech operations, the anticipated synergies did not materialize, leading to strategic shifts within Yahoo to optimise profitability and refocus on its core offerings (Fischer, 2023).

2.2 Nature of Business

According to Eckstein (2022), Yahoo initially offers a range of services such as search engines, email, and news feeds during its early years. However, with the rise of Google, which provided similar services more efficiently, Yahoo struggled to maintain its relevance and has since evolved into a collection of varied offerings. Despite these challenges, Yahoo continues to generate revenue primarily through the following services:

a. **Digital Advertising**: Following Apollo's acquisition, Yahoo has taken significant steps to streamline its operations by shutting down unprofitable units, including its supply-side platform (SSP) and native advertising platform (Gemini) (Fischer, 2023). The company is now focusing on its demand-side platform (DSP), which has been rebranded as Yahoo Advertising. This revamped strategy aims to target Fortune 500

companies and optimise ad revenue. Additionally, Yahoo has formed a new partnership with Taboola to enhance its advertising capabilities.

b. **Subscription Services**: Yahoo Finance launched Yahoo Finance Premium, a subscription service priced at $49.99 per month, offering users advanced analytics, research reports, and enhanced portfolio management tools (Eckstein, 2022).

c. **Yahoo Mail Updates**: The Yahoo Mail app has been enhanced into a "super-app" featuring a "Deals" tab that provides personalised shopping offers, with the goal of increasing ad revenue by leveraging user loyalty (Eckstein, 2022).

2.3 Organisational Structure

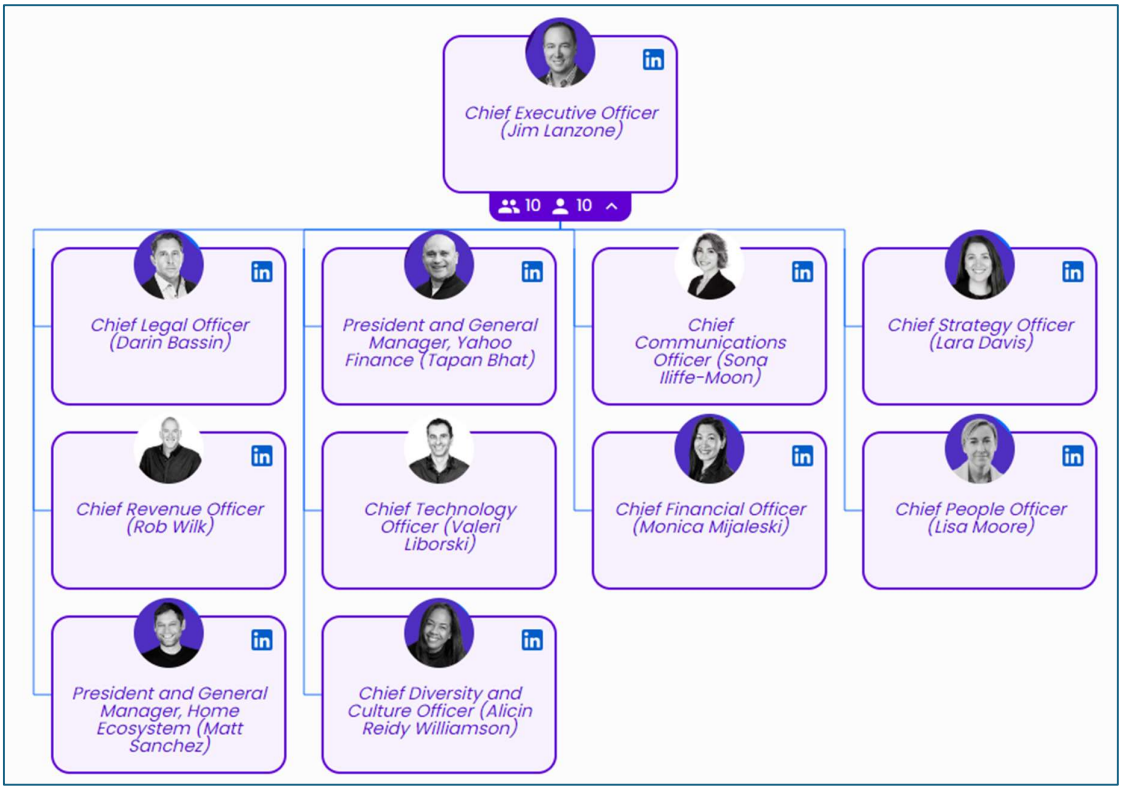
Yahoo's global operations are supported by a network of 24 offices across key regions: 11 in the Americas, 6 in Europe, and 7 in the Asia-Pacific (Yahoo, 2024). This extensive geographical footprint not only enhances Yahoo's global reach but also positions the company to better cater to the needs of its customers and partners worldwide.

In 2023, Yahoo underwent a significant restructuring of its advertising technology unit, leading to layoffs that will affect over 20% of its total workforce, which amounts to more than 1,600 employees (Fischer, 2023). Following these changes, the company is estimated to have around 8,000 employees (Goswami, 2023).

Moreover, Yahoo has an information security team known as the Paranoids, and the team is dedicated to enhancing the company's security culture (Pearlson et al., 2021). This team integrates various specialised groups, including a red team for offensive security testing, a security awareness team for employee education, and a behavioural engineering team that measures and analyses security behaviours. Pearlson et al. (2021) mentions that the Paranoids aim to foster a proactive and vigilant cybersecurity environment across the organisation by employing innovative strategies and data-driven insights.

Additionally, Yahoo is guided by an experienced management team, each bringing unique expertise from various sectors within technology and media (Yahoo, 2024). The leadership team is led by Jim Lanzone, the CEO, who has a distinguished track record in driving growth and innovation across several major technology companies. An organisational chart illustrating the leadership structure and key roles within the company is included under Figure 2 below, providing a visual representation of Yahoo's leadership team dynamics.

Figure 2: Yahoo's leadership team organisational chart



3.0 Yahoo's Current Information Security Design

This section outlines Yahoo's current approach to information security, focusing on its compliance with industry standards, the structure of its security program, and the foundational principles guiding its security framework.

3.1 Compliance Status

Yahoo is committed to maintaining compliance with various industry standards and regulatory requirements through its comprehensive information security program. Yahoo adheres to the following standards and regulations to ensure information security and compliance (Nir, 2023; Paranoids, 2022; Yahoo, n.d.; Yahoo, 2022):

a. **ISO 27001/27005**: Used for information security management and risk processes.
b. **NIST CSF**: Aligns security policies for threat detection and response.
c. **GDPR**: Enforces data privacy for EU users.
d. **HIPAA**: Protects sensitive healthcare information.
e. **PCI DSS**: Secures payment card data.
f. **SCCs**: Ensures compliance for international data transfers.

g. **NIST 800-30**: Guides risk assessments.
h. **NIST SP 800-53**: Secures data centers and physical environments.
i. **SOC2**: Evaluates internal controls for data security, availability, and confidentiality.

3.2 Information Security Program

Yahoo's information security program encompasses a comprehensive set of practices designed to protect its assets, data, and operations. This section highlights the important aspects of Yahoo's security measures, detailing how the company implements encryption, access control, and other essential strategies to safeguard its systems and maintain compliance with industry standards. Table 1 provides a summary of the security program.

Table 1: Security aspects and practices in Yahoo's information security program (Paranoids, 2022; Yahoo, n.d.; Yahoo, 2022)

Aspect	Practices
Encryption	Implements industry-standard encryption and mandates the use of TLS 1.2 or higher. Any non-compliant encryption methods must be reviewed and approved by the security department. Encrypts critical products and services. This includes securing traffic between data centers and defaulting to HTTPS for Yahoo Mail and other platforms. The company adheres to modern security best practices, supporting TLS 1.2 with 2048-bit RSA keys and utilising Forward Secrecy. Additionally, advanced protections such as HSTS, HPKP, OCSP Stapling, and Certificate Transparency are implemented.
Access control	Access to Yahoo's corporate systems is tightly controlled, with remote access requiring additional safeguards.
System development and maintenance	Reviews third-party vulnerabilities and remediates them based on business risk. They also conduct vulnerability assessments, code reviews, and operates a public bug bounty program to identify and address security issues proactively.

Incident response	Operates a Security Operations Center (SOC) that monitors security events and utilises a variety of technologies to detect, block, and remediate threats. The SOC has an established process for incident response, combined with regular training and updated threat intelligence, ensures a swift reaction to security incidents. Yahoo's incident response plan consists of preparation, detection, containment, eradication, recovery, and continuous improvement stages, with regular updates and third-party engagement as needed.
Organisational security	All employees must follow security practices and standards, while the information security team ensures compliance through policy enforcement, risk assessments, and security consulting. The team also designs and tests security solutions, manages operations, and coordinates incident response to protect organisational assets.
Physical and environmental security	Uses various security measures to protect physical infrastructure, including architectural controls and continuous monitoring of threats.
Personnel security	To mitigate insider threats, Yahoo implements comprehensive personnel security measures, including role-based access control (RBAC), multi-factor authentication (MFA), thorough background checks, and annual training on information security and data privacy for all employees and contractors.
Network security	Ensures robust access control for network devices by utilising a zero-trust model. Their network security strategy includes perimeter defense measures, standardizes configurations, implements secure change management, and conducts regular risk assessments.
Cloud security	Employs robust controls for cloud-hosted data, focusing on identity management, logging, secure networking, application protection, and data encryption.

Mobile security	Enforces strict policies and controls to address the risks associated with mobile devices. The measures include secure procedures for integrating third-party SDKs and requirements for mobile device management (MDM).

In summary, Yahoo's comprehensive information security practices reflect a proactive and layered approach to safeguarding its digital assets and maintaining the trust of its users.

3.3 Security Design Framework and Architecture Principles

This section delves into the fundamental principles that underline Yahoo's security design framework. By focusing on key areas such as asset management, risk management, vulnerability management, and compliance adherence, it outlines how these components collectively contribute to a comprehensive and effective security framework. The components of the framework are described under Table 2.

Table 2: Principles of Yahoo's security design framework (Paranoids, 2022; Yahoo, n.d.; Yahoo, 2022)

Principle	Implementation
Asset classification and control	Maintains a system to track physical and logical assets such as databases, software, and devices. Assets are classified based on business criticality, and safeguards like access management and encryption are applied as needed.
Risk management	Adopts a risk-driven strategy, identifying potential threats and vulnerabilities through formal assessments aligned with NIST 800-30. Their process includes system characterisation, risk identification, impact analysis, probability calculations, controls examination, and risk prioritisation. Findings are reported to executive leadership for timely remediation.
Vulnerability management	A dedicated team manages vulnerability identification and remediation, conducting regular scans and maintaining up-to-date software to address newly disclosed vulnerabilities.

Operations management	Changes to systems, infrastructure, and applications are controlled via a centralised change management system, which includes impact analysis and testing.
Business continuity planning	To minimise service disruptions, Yahoo's business continuity program features global redundancy, continuous monitoring, and a dedicated governance team for plan oversight.
Secure software development	Integrates security throughout the software development lifecycle by emphasising "Secure by Design." This approach involves incorporating security requirements during the planning phase, providing secure coding training for developers, and conducting comprehensive testing along with final checks before the software release.
Compliance and governance	Maintains a strong information security policy framework aligned with industry standards such as NIST CSF, GDPR, HIPAA, and PCI DSS regularly reviewed by their "Paranoids" team. In addition, Yahoo's security, legal, and privacy departments collaborate to ensure compliance with regional laws and regulations. This is supported by regular internal and external assessments, security consulting, and risk management processes.
Transparency	Commits to promptly inform users of suspected state-sponsored attacks and provides resources for fraud prevention, including personalised security tips. In the event of a breach, affected users are notified via email and in-app alerts, with passwords reset if unauthorised access is suspected. The incident response team quickly assesses potential data compromises, working to contain the issue while ensuring timely notifications to regulators and users.

In summary, Yahoo's comprehensive security design framework not only prioritises asset classification and risk management but also emphasises a proactive approach to vulnerability and operations management. By embedding security into the software development lifecycle and maintaining transparency with users, Yahoo demonstrates a commitment to robust security practices.

4.0 Yahoo's Information Security Issues and Vulnerabilities

Yahoo has faced several security challenges, including data breaches that exposed significant vulnerabilities. This section reviews both past and current security issues, focusing on key incidents and weaknesses that have affected Yahoo's operations. It also examines the present cybersecurity risks the company faces in today's evolving threat landscape.

4.1 Major Security Incidents

In 2013 and 2014, Yahoo suffered two of the largest data breaches in history, impacting billions of users and exposing significant vulnerabilities within the company's security practices (Trautman & Ormerod, 2016). Both breaches, which involved the exposure of names, email addresses, phone numbers, birth dates, as well as both encrypted and unencrypted security questions, were not publicly disclosed until September 2016, despite Yahoo being aware of at least one of them much earlier.

The first incident, a 2013 data breach, was disclosed in December 2016 and compromised the personal information of all three billion user accounts on Yahoo's servers. (Haselton, 2017). This breach was linked to an unauthorised third-party accessing Yahoo's servers (Zhang et al., 2022). Yahoo only became aware of the breach when it received data files from law enforcement, highlighting that the company was unaware of the scale of the incident for several years (Trautman & Ormerod, 2016).

In 2014, another breach compromised the personal information of over 500 million user accounts, though it was not publicly revealed until September 2016 (Trautman & Ormerod, 2016). This breach was attributed to weak encryption practices (Zhang et al., 2022). Although Yahoo initially blamed a state-sponsored actor, later investigations pointed to a cybercrime group and even suggested internal involvement. The attack was initiated through spear-phishing emails that delivered malware, when clicked by employees, spread across Yahoo's network, granting unauthorised access to emails and internal systems. Trautman and Ormerod (2016) mentions that the investigations also revealed that Yahoo's security team had knowledge of the breach as early as 2014, including incidents of cookie forging in 2015 and 2016. Unfortunately, this information was not effectively communicated to senior management at the time.

These events highlighted Yahoo's inadequate security measures and underscored the need for stronger policies, improved detection systems, and comprehensive employee cybersecurity training to prevent similar incidents in the future.

4.2 Issues and Vulnerabilities in Yahoo's Security Practices

4.2.1 Past Issues and Vulnerabilities

According to Trautman and Ormerod (2016), the 2013 and 2014 breaches exposed several weaknesses in Yahoo's security practices:

a. **Usability and Profitability Over Security:** The leadership team prioritised user experience and revenue generation over robust security measures, ignoring internal security team warnings. The previous CEO, Marrisa Mayer's resistance to implementing end-to-end encryption due to concerns about limiting user data analysis demonstrated this mindset, creating a culture where security was seen as a secondary concern.

b. **Insufficient Cybersecurity Investment**: Yahoo failed to adequately allocate resources for essential security needs, including personnel and technology, leading to a reactive rather than proactive security approach. The Paranoids often faced resistance in securing resources, and the delayed implementation of a bug bounty program compared to competitors underscored this lack of investment.

c. **Poor Internal Communication and Reporting**: There was a significant disconnect between the security team and senior management, resulting in inadequate risk assessment and response to security threats. Information regarding the 2014 breach took nearly two years to reach senior management, highlighting failures in communication and internal reporting structures.

d. **Inadequate Monitoring and Incident Response:** The 2013 data breach, affecting over 1 billion accounts, went undetected for years, only coming to light when law enforcement provided stolen data. While Yahoo claims to have established a Security Operations Center (SOC) and incident response plans, their past shortcomings raise questions about the effectiveness of these measures.

e. **Inadequate Response to Previous Incidents:** Yahoo's response to the 2010 breach involving Chinese military hackers was considerably slower and less robust than competitors like Google.

Another major issue was the company's reliance on outdated cryptographic practices (Menn et al., 2016). User passwords were encrypted using the outdated and insecure MD5 algorithm, while certain security questions were left unencrypted (Nelson, 2024). Although

Yahoo attempted to phase out the insecure MD5 encryption method in 2013, this effort came too late, as hackers compromised billions of accounts that year (Menn et al., 2016). Despite warnings from security experts since 2008, Yahoo continued using MD5 until the breach occurred, resulting in inadequate encryption that could have been significantly strengthened with modern hashing algorithms.

Furthermore, Yahoo faced criticism for its lack of commitment to safeguarding user data and addressing corporate security concerns (Nelson, 2024). This issue was highlighted by the company's short-lived tenure with Alex Stamos, hired as Chief Security Officer (CSO) in 2014. Despite being brought on to revamp Yahoo's security, Stamos resigned after discovering that the CEO had secretly authorised software allowing federal officials to read users' emails, reflecting a broader governance failure at the company. This situation mirrors the struggles many organisations face today in balancing security with internal politics and governance.

4.2.2 Current Issues and Vulnerabilities

According to a vendor risk report by UpGuard (2024), Yahoo faces several security vulnerabilities across its systems:

a. **Website Security**: The Content Security Policy (CSP) is implemented unsafely, allowing 'unsafe-inline' without a nonce or hash, which could expose the site to XSS attacks.

b. **Email Security**: Yahoo's Sender Policy Framework (SPF) uses the 'ptr' mechanism, which should only be used temporarily. Prolonged use places unnecessary strain on DNS servers and risks mail checkers ignoring the SPF record.

c. **DNS**: DNS Security Extensions (DNSSEC) are not enabled, leaving the domain vulnerable to record forgery that could compromise its identity.

d. **Encryption**: Several encryption-related vulnerabilities were identified, including support for insecure SSL/TLS versions, a soon-to-expire SSL certificate, weak cipher suites in TLS 1.2, and the absence of essential HTTP Strict Transport Security (HSTS) protections. Additionally, the domain is missing from the HSTS preload list, making first-time visitors susceptible to man-in-the-middle (MITM) attacks.

Furthermore, a recent research by SquareX revealed critical flaws in Yahoo Mail's attachment scanning (Winder, 2024). The study found that Yahoo failed to block a malicious file disguised as a PowerPoint presentation, which was detected by 40 virus scanners.

Moreover, a malicious Excel document bypassed security measures, with no alerts issued to users, unlike Gmail, which provided warnings for similar threats.

4.3 Potential Cybersecurity Risks and Threats

Today, Yahoo may face various critical cybersecurity risks, particularly those related to its web applications. These vulnerabilities can have serious implications for the integrity, availability, and confidentiality of its online services. The OWASP Top Ten is a widely recognised framework that identifies the most critical security risks to web applications (OWASP, 2021). The potential impacts of the OWASP Top Ten risks on Yahoo's information security are summarized under Table 3.

Table 3: OWASP top 10 security risks of web application and their impacts (OWASP, 2021)

Risks	**How Yahoo may be affected**
Broken access control	The prevalence of broken access control vulnerabilities could lead to unauthorised access to sensitive user data and critical systems within Yahoo, damaging user trust and compliance.
Cryptographic failures	Weaknesses in cryptographic implementations could expose Yahoo's sensitive data to interception or compromise, leading to severe data breaches and potential regulatory penalties.
Injection	Injection vulnerabilities, including cross-site scripting, could allow attackers to manipulate Yahoo's applications, potentially leading to data theft, service disruption, or unauthorised actions on behalf of users.
Insecure design	Flaws in the design of Yahoo's systems could introduce inherent security weaknesses that make it easier for attackers to exploit vulnerabilities and compromise user data.
Security Misconfiguration	Misconfigurations within Yahoo's applications or infrastructure may create security gaps, allowing attackers to exploit these weaknesses to gain unauthorised access to systems and data.
Vulnerable and outdated components	The use of outdated software components can leave Yahoo vulnerable to known exploits, potentially leading to system breaches and data exposure if not properly managed.

Identification and authentication failures	Failures in identification and authentication mechanisms could allow unauthorised users to gain access to Yahoo's systems, undermining the integrity of user accounts and sensitive information.
Software and data integrity failures	Assumptions about the integrity of software updates and critical data without verification could expose Yahoo to risks where malicious code is introduced into their systems, resulting in data corruption or breaches.
Security logging and monitoring failures	Insufficient logging and monitoring can hinder Yahoo's ability to detect and respond to security incidents promptly, increasing the impact and duration of potential breaches.
Server-side request forgery	Server-side request forgery vulnerabilities could allow attackers to make unauthorised requests from Yahoo's servers, potentially leading to data leaks or further compromise of internal services.

Additionally, SentinelOne (2024) mentions that organisations will encounter a range of significant cybersecurity threats that can compromise their operations and data security. Yahoo, as a prominent digital entity, may be particularly vulnerable to these threats. Key threats in 2024 include (SentinelOne, 2024):

a. **Social Engineering**: Attackers exploit human psychology to manipulate individuals into sharing sensitive information, often through phishing scams or deceptive communication.

b. **Ransomware**: This type of malware locks users out of their data, demanding a ransom for access restoration. Ransomware attacks can lead to severe financial losses and operational disruptions.

c. **Insider Threats**: Employees or contractors may unintentionally or maliciously cause data breaches. Identifying these threats is challenging since they stem from trusted individuals within the organisation.

d. **Third-Party Exposure**: Risks associated with third-party vendors can compromise an organisation’s data security if those vendors have inadequate protective measures.

e. **Artificial Intelligence Cyber Threats**: Cybercriminals leverage AI to enhance the sophistication of their attacks, including automating phishing campaigns and discovering system vulnerabilities.

f. **Configuration Mistakes**: Poorly configured systems and applications can create vulnerabilities that be exploited, such as leaving sensitive data publicly accessible.

a. **State-Sponsored Attacks**: Cyber operations conducted by nation-states aim at political, military, or economic gains and often employ advanced techniques that pose significant threats to national and corporate security.

5.0 Proposed Improvements to Yahoo's Security Design

This section outlines the proposed improvements to Yahoo's existing information security design. It identifies the key security gaps and vulnerabilities highlighted in the previous sections and presents targeted solutions to address these issues. Each recommendation is designed to mitigate current risks and future threats, ensuring a more resilient and secure environment for Yahoo's operations.

5.1 Identifying Security Gaps

In order to strengthen Yahoo's overall information security posture, it is essential to identify and address the existing gaps in its current security design. These gaps, derived from both the organisation's structure and historical security issues, provide valuable insight into areas where Yahoo's security framework falls short. Table 4 below highlights the specific design gaps within Yahoo's current information security design and the related issues discussed earlier.

Table 4: Gap in Yahoo's information security design based on organisational information and issues discussed

Weakness	Gap in Current Design	Issues Discussed Regarding the Design's Weaknesses
Usability and Profitability Prioritised Over Security	Lack of emphasis on balancing usability with robust security measures.	**A)** Leadership prioritised user experience and profitability over security. **B)** Delayed critical security features. **C)** Created a reactive security culture rather than proactive.
Insufficient Cybersecurity Investment	No mention of consistent resource allocation or	**A)** Struggled to secure adequate resources for the security team.

	scaling of the security team according to growing needs.	**B)** Underinvestment impacted vulnerability management and threat response. **C)** Delayed adoption of bug bounty programs and other security upgrades.
Weak Encryption Practices and Delayed Upgrades	Employs standard encryption but lacks clear emphasis on upgrading or phasing out older methods quickly.	**A)** Continued using insecure encryption despite warnings. **B)** Slow upgrade process allowed vulnerabilities to persist. **C)** Proactive replacement of insecure practices was lacking.
Poor Internal Communication and Incident Response	No specific mention of improving communication between security teams and management.	**A)** Communication failures delayed breach reporting to senior management. **B)** Highlighted weaknesses in internal processes for relaying critical security risks.
Inadequate Monitoring and Detection	Has a SOC, but no specific mention of improving monitoring tools and real-time threat detection.	**A)** Monitoring systems failed to detect major breaches. **B)** Detection issues were only identified after law enforcement involvement. **C)** Need for better real-time detection capabilities.
Ineffective Vulnerability and Patch Management	Vulnerability management and patching are described, but lacks emphasis on rapid patch deployment or vulnerability remediation.	**A)** Delays in patching known vulnerabilities allowed attackers to exploit weaknesses. **B)** Outdated cryptographic standards persisted without timely updates.
Website and Email Security Issues	No specific mention of continuous website and email security hardening beyond general encryption and access control practices.	**A)** Unsafe Content Security Policy (CSP) configurations. **B)** Weaknesses in Yahoo Mail's security scanning. **C)** Flawed SPF record setups, leaving email security vulnerable.

Insufficient Focus on Insider Threats	Personnel security is described, but lacks emphasis on detecting or preventing insider threats.	**A)** Potential involvement of insiders in past breaches. **B)** Gaps in employee training, particularly around phishing risks. **C)** Lack of development in internal threat detection measures.

5.2 Solutions to Address Gaps

In response to the identified weaknesses within Yahoo's information security framework, this section outlines targeted solutions designed to mitigate each gap. Each gap will be addressed individually, detailing the proposed strategies and their potential impact on strengthening Yahoo's overall information security program.

5.2.1 Gap 1: Lack of Emphasis on Balancing Usability with Robust Security Measures

According to Licel (2023), there are several ways to achieve a balance between security and usability. Several improvements are proposed to address the design gap (Licel, 2023):

a. **Layered Security**: Employ multi-layered security strategies, integrating robust measures like transport layer security (TLS) and data-at-rest encryption (e.g., AES). These layers should operate in the background to avoid overwhelming users with prompts.
b. **User-Centric Design**: Implement intuitive authentication methods, such as biometric verification, and streamline processes to enhance usability without sacrificing security.
c. **Behavioural Analytics**: Utilise analytics to monitor typical user behavior, enabling the detection of anomalies and reducing friction during normal operations.
d. **Customisation Options**: Allow users to customise security settings, fostering a sense of control while ensuring strong default protections.
e. **Transparency and Education**: Clearly communicate security protocols during onboarding and provide resources that help users understand security features. This can build trust and enhance user engagement.

To bridge the gap between usability and robust security measures while managing compliance, organisations should adopt both usability and compliance testing (Temby, n.d.). Temby (n.d.) mentions that compliance testing assesses an organisation’s adherence to standards and guidelines. Since Yahoo has not explicitly stated whether it conducts compliance

testing, the extent of its adherence to accessibility guidelines remains unclear. To strengthen its security design, Yahoo should integrate both usability and compliance testing, ensuring alignment with relevant policies and industry standards while simultaneously enhancing the overall user experience.

5.2.2 Gap 2: No Mention of Consistent Resource Allocation or Scaling of the Security Team

To enhance resource allocation for security and effectively scale the security team, Yahoo should consider several strategies based on insights from industry best practices:

a. **Establish a cybersecurity budget aligned with risk:** Yahoo should form a cross-organisational management team, appointed by the board, to develop a cybersecurity budget that reflects identified risks (Mack & Bloom, 2017). This involves:
    - Conducting comprehensive risk assessments to identify potential cyber threats and vulnerabilities.
    - Aligning the budget with the organisation's risk appetite to prioritise critical security areas, such as threat detection and incident response.

b. **Implement automation and technology to optimise resources**: Leveraging technological solutions can enhance security measures. Yahoo should:
    - Automate routine security operations, such as vulnerability scanning and log analysis, to allow security personnel to focus on strategic initiatives (World Economic Forum, 2024).
    - Enhance threat detection and response capabilities through AI-powered tools and advanced security technologies, minimising the workload on security analysts (Zhang et al., 2022).
    - Utilise cloud security tools for automated security assessments and compliance monitoring in cloud environments (Cisco, 2024).

c. **Foster a culture of security awareness**: World Economic Forum (2024) highlights the importance of user awareness. Yahoo should:
    - Develop ongoing security awareness programs to educate employees on best practices, including phishing and password security.
    - Encourage a security-first mindset, empowering employees to view security as a collective responsibility and report incidents promptly.
    - Integrate security awareness training into onboarding processes and provide regular refreshers to reinforce best practices.

By implementing these strategies, Yahoo can improve its resource allocation and effectively scale its security team, ensuring robust compliance with industry standards while adapting to evolving security threats. A well-resourced and flexible security program is crucial for protecting Yahoo's users, data, and reputation.

5.2.3 Gap 3: Employs Standard Encryption but Lacks Emphasis on Upgrading or Phasing Out Older Methods Quickly

To enhance its encryption practices, Yahoo must adopt a proactive approach that prioritises upgrading and phasing out outdated encryption methods. Key strategies include:

a. **Establish an encryption policy lifecycle**: Yahoo should implement a structured lifecycle for its encryption policies that encompasses:
   - Regular reviews and updates through annual assessments of encryption policies to stay aligned with the evolving threat landscape and industry best practices, incorporating new encryption algorithms and technologies (Zhang et al., 2022).
   - Sunset plans for outdated encryption by developing a clear roadmap for phasing out older encryption methods, identifying systems utilising outdated algorithms, evaluating the associated risks, and outlining strategies for migration to more secure options (Cisco, 2024).
   - A key management lifecycle that covers key generation, distribution, rotation, and destruction, with a focus on secure storage and adherence to industry standards (Cuevas et al., 2015).

b. **Prioritising strong encryption for sensitive data**: Yahoo should take steps to protect sensitive information by:
   - Identifying and classifying sensitive data through a thorough data inventory to classify information based on sensitivity, guiding decisions on encryption strength and access control (Zhang et al., 2022).
   - Implementing end-to-end encryption for sensitive data during transmission and storage, ensuring that even in the event of a breach, data remains protected without the proper decryption keys (Zhang et al., 2022).
   - Evaluating modern encryption algorithms by regularly assessing and adopting modern encryption standards, such as Advanced Encryption Standard (AES) with suitable key lengths, while moving away from outdated algorithms.

c. **Recovery strategies and compliance management**: Yahoo should enhance its recovery and compliance strategies by:
    - Developing a data recovery plan that creates a robust plan to recover encrypted data in case of system failures or security incidents, which includes secure key backups and testing procedures to ensure effective recoverability (Microsoft, 2017).
    - Maintaining regulatory compliance to ensure adherence to relevant data protection regulations, including GDPR and CCPA, as well as industry standards like PCI DSS, particularly regarding data encryption and breach notification protocols (Zhang et al., 2022).
    - Engaging in external security audits through regular third-party audits to evaluate encryption practices, identify vulnerabilities, and ensure compliance with regulatory requirements and industry best practices (Zhang et al., 2022).

By implementing these measures, Yahoo can address its reliance on standard encryption practices and improve its overall security posture, thereby enhancing data protection and building user trust in its online services.

5.2.4 Gap 4: No Specific Mention of Improving Communication Between Security Teams and Management

To strengthen communication between security teams and management, Yahoo can implement strategies that enhance collaboration and information sharing. Key recommendations include:

a. **Establish clear communication channels** (Mack & Bloom, 2017): Yahoo should prioritise regular interactions between security teams and management by:
    - Implementing structured reporting schedules for security teams to present key metrics, ongoing initiatives, and emerging threats through weekly or monthly updates, along with urgent briefings during critical incidents.
    - Utilising dedicated collaboration tools to facilitate secure information sharing and communication, creating specific channels for incident response and policy updates.
    - Appointing communication liaisons within the security team to tailor information for various management levels, ensuring that communications are relevant and comprehensible.

b. **Develop a common language and reporting framework** (Mack & Bloom, 2017): To enhance understanding between security teams and management, Yahoo can:
    - Create a cybersecurity glossary that defines relevant terms and concepts to ensure consistent terminology and understanding across teams.
    - Standardise reporting formats to present security metrics, risk assessments, and incident summaries in a uniform manner, simplifying information interpretation for management.
    - Train security teams to articulate security issues in terms of business impact, aligning their communication with the organisation's operational, financial, and reputational concerns.

By adopting these strategies, Yahoo can significantly improve communication between its security teams and management. This enhanced collaboration will empower the organisation to proactively address vulnerabilities, respond effectively to security incidents, and strengthen its overall security posture while ensuring compliance with relevant standards.

5.2.5 Gap 5: Has a SOC, but No Specific Mention of Improving Monitoring Tools and Real-Time Threat Detection

To enhance its Security Operations Center (SOC) capabilities, Yahoo should focus on upgrading monitoring tools and improving real-time threat detection. Key proposals include:

a. **Upgrade monitoring tools**: Yahoo can strengthen its security posture by implementing advanced monitoring solutions, including:
    - User and Entity Behavior Analytics (UEBA) to establish baselines for normal behavior and detect deviations indicative of potential threats. Implementing UEBA will help identify insider threats and support compliance by proactively monitoring user activities (Microsoft, 2017).
b. **Enhance real-time threat detection**: Yahoo should focus on integrating advanced threat detection measures, including:
    - Automated threat response through Security Orchestration, Automation, and Response (SOAR) capabilities. Utilising SOAR platforms will streamline incident response workflows, allowing for quick actions in response to detected threats, minimising downtime, and ensuring compliance through consistent response actions (IBM, n.d.).

c. **Provide security skills and training for SOC analysts**: Equip them with advanced threat detection and incident response skills, addressing the growing concern over skill gaps in cybersecurity (Microsoft, 2017).
d. **Perform regular testing and evaluation of monitoring tools and response procedures** (Microsoft, 2017): This can be done through security assessments and red team exercises. Continuous evaluation will identify weaknesses and enhance the SOC's adaptability to evolving threats.

By implementing these recommendations, Yahoo can significantly enhance its SOC capabilities, ensuring effective real-time threat detection and response. This will protect user data, maintain business continuity, and build trust in Yahoo's services while also aligning with compliance requirements.

5.2.6 Gap 6: Lack Emphasis on Rapid Patch Deployment or Vulnerability Remediation

To address weaknesses in vulnerability management and patching at Yahoo, a focus on rapid deployment and remediation is essential. Key approaches include:

a. **Accelerate patch deployment**: A robust patch management solution is necessary to automate the deployment process across Yahoo's infrastructure (Aboelfotoh & Hikal, 2019). Automating patching can significantly decrease remediation time and reduce the exposure window for attackers. Rapid patch deployment is vital for mitigating the impact of vulnerabilities and streamlining recovery efforts while ensuring compliance with various frameworks, such as PCI DSS and HIPAA.
b. **Establish Service Level Agreements (SLAs)**: Clearly defined SLAs for vulnerability remediation should be implemented, specifying timelines based on the severity of vulnerabilities (Alibha, 2024). High-risk vulnerabilities should be addressed the quickest. These SLAs will ensure timely action, minimise operational disruptions, and demonstrate a commitment to security, which is essential for compliance with audit requirements.
c. **Address legacy systems**: An inventory of legacy systems that may not support automated patching is critical (Das, 2024). A plan should be developed to mitigate risks associated with these systems, such as through network segmentation or phased upgrades. Addressing vulnerabilities in legacy technology is crucial for recovery, as it offers alternative remediation strategies and helps maintain compliance with regulations that mandate managing known vulnerabilities.

By implementing these strategies, Yahoo can enhance its vulnerability management and patching processes, focusing on rapid deployment and remediation. This proactive stance will fortify Yahoo's security framework, reduce the likelihood of successful attacks, and protect user data effectively.

5.2.7 Gap 7: No Specific Mention of Continuous Website and Email Security Hardening

To address the lack of emphasis on continuous website and email security hardening at Yahoo, the following comprehensive strategies are proposed:

a. **Implement a continuous security monitoring program**: Utilising Web Application Firewalls (WAFs) on top of having a SIEM can provide an extra layer of protection against common web vulnerabilities (Cloudflare, n.d.). Continuous monitoring allows for real-time threat detection, thereby reducing the likelihood of successful breaches and aligning with compliance requirements like PCI DSS and HIPAA.
b. **Automate website and email security hardening tasks**: Automated vulnerability scanning tools specifically designed for web applications and email servers should be integrated into a Continuous Integration/Continuous Delivery (CI/CD) pipeline (OWASP, n.d.). This approach will help identify vulnerabilities and misconfigurations early in the development process, ensuring that security hardening is an ongoing priority. Automating these tasks minimises human error and expedites recovery during security incidents, while also supporting compliance with industry standards.
c. **Establish a patch management process for third-party components** (Jackins, 2024)**:** Developing a robust process for identifying and tracking third-party software used in website and email systems is crucial. This process should ensure timely security updates for components like content management systems, plugins, and libraries. Effectively managing third-party risks will mitigate vulnerabilities that could be exploited by attackers, facilitating quicker recovery and compliance with vulnerability management regulations.

5.2.8 Gap 8: Personnel Security Lacks Emphasis on Detecting or Preventing Insider Threats

To enhance personnel security at Yahoo, particularly in relation to insider threats, the following strategies are recommended:

a. **Implement a comprehensive insider threat program**: Establishing a formal insider threat program is critical, covering all stages of the employee lifecycle from recruitment to offboarding. This program should include well-defined policies, procedures, and

training initiatives to manage insider risks effectively (Exabeam, n.d.). By applying the broader principles of security governance outlined in existing sources, this program will significantly strengthen Yahoo's overall security posture.

b. **Implement a zero trust security model with Privileged Access Management (PAM)** (ManageEngine, 2024): Transitioning to a Zero Trust model is critical, operating on the principle of "never trust, always verify." This requires continuous verification of users and devices before granting access. Incorporating a robust PAM solution is essential for managing privileged access, including enforcing strong authentication methods, implementing just-in-time access, and regularly auditing privileged access rights to reduce the risk of insider threats effectively.

c. **Establish clear data handling policies and procedures with comprehensive monitoring** (Rawat, 2024): Developing clear policies governing the access, use, storage, and transmission of sensitive data is paramount. This should be complemented by implementing a formal data classification scheme to dictate security controls based on data sensitivity. Utilising data loss prevention (DLP) solutions and security information and event management (SIEM) systems enables organisations to monitor data movement and aggregate security logs for centralized visibility.

These steps will help strengthen personnel security and improve defenses against insider threats while ensuring compliance with relevant regulations.

6.0 Conclusion

This report has provided a comprehensive analysis of Yahoo's information security landscape, focusing on the organisation's inherent vulnerabilities and the structural weaknesses that have emerged from past security incidents. By delving into Yahoo's business nature, organisational structure, and current compliance frameworks, it has become evident that the company is navigating a complex cybersecurity environment that necessitates urgent and strategic improvements.

Through the examination of Yahoo's current information security design, several critical gaps are identified. These weaknesses are compounded by a rapidly evolving threat landscape, requiring Yahoo to adopt a more proactive and resilient security posture. To address these identified weaknesses, targeted improvements have been proposed. These recommendations are designed to strengthen Yahoo's overall security framework, align with

regulatory compliance requirements, and ultimately protect sensitive user data from potential breaches.

In conclusion, Yahoo's commitment to evolving its information security practices is crucial for not only mitigating current risks but also for fostering trust with users and stakeholders. By prioritising the proposed solutions, Yahoo can enhance its information security design, safeguard against emerging cyber threats, and establish itself as a leader in cybersecurity within the digital landscape. This proactive approach is essential for ensuring the organisation's long-term viability and resilience in a competitive and increasingly challenging environment.

7.0 References

Aboelfotoh, S. F., & Hikal, N. A. (2019). A Review of Cyber-security Measuring and Assessment Methods for Modern Enterprises. *JOIV : International Journal on Informatics Visualization*, *3*(2), 157–176. https://doi.org/10.30630/joiv.3.2.239

Alibha. (2024, May 13). *Service Level Agreements (SLA) for vulnerability management*. Strobes. https://strobes.co/blog/service-level-agreements-sla-for-vulnerability-management/#:~:text=An%20SLA%20provides%20guidelines%20on,reducing%20the%20overall%20security%20risk.

Apollo Global Management. (2021, September 1). *Apollo funds complete acquisition of Yahoo*. https://www.apollo.com/insights-news/pressreleases/2021/09/apollo-funds-complete-acquisition-of-yahoo-161530593

Cisco. (2024). 2024 *Cisco cybersecurity readiness index*. https://newsroom.cisco.com/c/dam/r/newsroom/en/us/interactive/cybersecurity-readiness-index/documents/Cisco_Cybersecurity_Readiness_IND.pdf

Cloudflare. (n.d.). *What is a WAF? | web application firewall explained*. https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/

Cuevas, A., McCollom, A., Barczynski, J., Kretzer, K., Brady, C., & Doberstein, M. (2015). Policy Paper: Standardized Data Breach Reports.

Das, D. (2024, July 17). *Do legacy applications or operating systems cause gaps in your vulnerability management strategy? Microsegmentation can help*. ColorTokens. https://colortokens.com/blogs/do-legacy-applications-or-operating-systems-cause-gaps-in-your-vulnerability-management-strategy-microsegmentation-can-help/

Eckstein, J. (2022, December 7). *How Yahoo makes money*. Investopedia. https://www.investopedia.com/articles/markets/121015/how-yahoo-makes-money-yhoo.asp

Exabeam. (n.d.). *Insider threat programs: 8 tips to build a winning program*. https://www.exabeam.com/explainers/insider-threats/insider-threat-programs-8-tips-to-build-a-winning-program/

Fischer, S. (2023, February 9). *Exclusive: Yahoo to lay off more than 20% of staff as it*

shrinks ad biz. Axios. https://www.axios.com/2023/02/09/yahoo-layoffs-2023-tech-media-companies

Goswami, R. (2023, February 9). *Yahoo to lay off 20% of staff by year-end, beginning this week*. CNBC. https://www.cnbc.com/2023/02/09/yahoo-will-lay-off-nearly-1000-employees-by-end-of-2023.html

Haselton, T. (2017, October 3). *Yahoo just said every single account was affected by 2013 attack — 3 billion in all*. CNBC. https://www.cnbc.com/2017/10/03/yahoo-every-single-account-3-billion-people-affected-in-2013-attack.html

IBM. (n.d.). *What is SOAR (security orchestration, automation and response)?*. https://www.ibm.com/topics/security-orchestration-automation-response

Jackins, T. (2024, September 11). *Ultimate guide to 3rd party patch management*. Splashtop. https://www.splashtop.com/blog/ultimate-guide-3rd-party-patch-management#:~:text=Third%2Dparty%20patch%20management%20is,operating%20system%20or%20hardware%20manufacturer.

Licel. (2023, September 12). *Balancing security and usability*. https://licelus.com/insights/balancing-security-and-usability

Mack, O. V., & Bloom, K. (2017, November 27). *Yahoo's 10K: lessons on what not to do in a breach*. ACC Docket. https://docket.acc.com/yahoos-10k-lessons-what-not-do-breach

ManageEngine. (2024, May 17). *Zero Trust privileged access management*. https://www.manageengine.com/privileged-access-management/what-is-zero-trust-pam.html

Menn, J., Finkle, J., & Volz, D. (2016, December 19). *Yahoo security problems a story of too little, too late*. Reuters. https://www.reuters.com/article/technology/yahoo-security-problems-a-story-of-too-little-too-late-idUSKBN1480AM/

Microsoft. (2017). *Incident response reference guide*. https://learn.microsoft.com/en-us/microsoft-365/downloads/ir-reference-guide.pdf?view=o365-worldwide

Nelson, N. (2024, January 2). *10 years after yahoo breach, what's changed? (not much)*. Dark Reading. https://www.darkreading.com/cyberattacks-data-breaches/10-years-after-yahoo-whats-changed-not-much

Nir, O. (2023, February 2). *The complete list of data security standards*. Reflectiz. https://www.reflectiz.com/blog/data-security-standards/#:~:text=Security%20standards%20are%20a%20set,Standards%20and%20Technology%20(NIST).

OWASP. (n.d.). *Vulnerability scanning tools*. https://owasp.org/www-community/Vulnerability_Scanning_Tools

OWASP. (2021). *OWASP top ten*. https://owasp.org/www-project-top-ten/

Paranoids. (2022). *Yahoo information security*. https://assets.website-files.com/62b4f04befbe455f681f5197/62c4816017c8aad0d33781ce_yahoo-paranoids-information-security.pdf#page=3.20

Pearlson, K., Sposito, S., Arbisman, M., & Schwartz J. A. (2021, September 30). *How Yahoo built a culture of cybersecurity*. Harvard Business Review. https://hbr.org/2021/09/how-yahoo-built-a-culture-of-cybersecurity

Rawat, P. (2024, August 13). *Data handling policy & its advantages*. Infosec Train. https://www.infosectrain.com/blog/data-handling-policy-its-advantages/#:~:text=A%20comprehensive%20data%20handling%20policy,that%20it%20is%20obtained%20lawfully.

SentinelOne. (2024, August 28). *Top 11 cyber security threats in 2024*. https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-threats/

Temby, S. (n.d.). *Understanding usability testing and compliance testing*. iSoftStone. https://www.isoftstoneinc.com/insights/usability-compliance-testing/#:~:text=Usability%20testing%20assesses%20general%20usability,specifically%20recruits%20people%20with%20disabilities.

Tikkanen, A. (2017). *Yahoo! | History, sale & facts*. Britannica Money. https://www.britannica.com/money/Yahoo-Inc

Trautman, L. J., & Ormerod, P. C. (2016). Corporate directors' and officers' cybersecurity standard of care: The Yahoo data breach. *Am. UL Rev.*, 66, 1231.

UpGuard. (2024, September 27). *Yahoo! Security rating, vendor risk report, and data breaches.* https://www.upguard.com/security-report/yahoo

Winder, D. (2024, April 5). *Critical security flaws found in email top 4—Apple, Gmail, Outlook & Yahoo*. Forbes. https://www.forbes.com/sites/daveywinder/2024/04/04/critical-security-flaw-in-apple-icloud-google-gmail-microsoft-outlook-yahoo-mail-aol-mail-email/

World Economic Forum. (2024). *Global cybersecurity outlook 2024*. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

Yahoo. (n.d.). *Put consumers first*. https://www.yahooinc.com/transparency/about/put-consumers-first.html

Yahoo. (2022, December 5). *Yahoo technical and organisational security measures*. https://legal.yahoo.com/ie/en/yahoo/terms/securitymeasures/index.html

Yahoo. (2024). *About*. https://www.yahooinc.com/about

Yahoo. (2024). *Office locations*. https://www.yahooinc.com/office-locations

Zhang, X., Yadollahi, M. M., Dadkhah, S., Isah, H., Le, D.-P., & Ghorbani, A. A. (2022). Data breach: Analysis, countermeasures, and challenges. *International Journal of Information and Computer Security*, 19(3/4), 402. https://doi.org/10.1504/IJICS.2022.127169