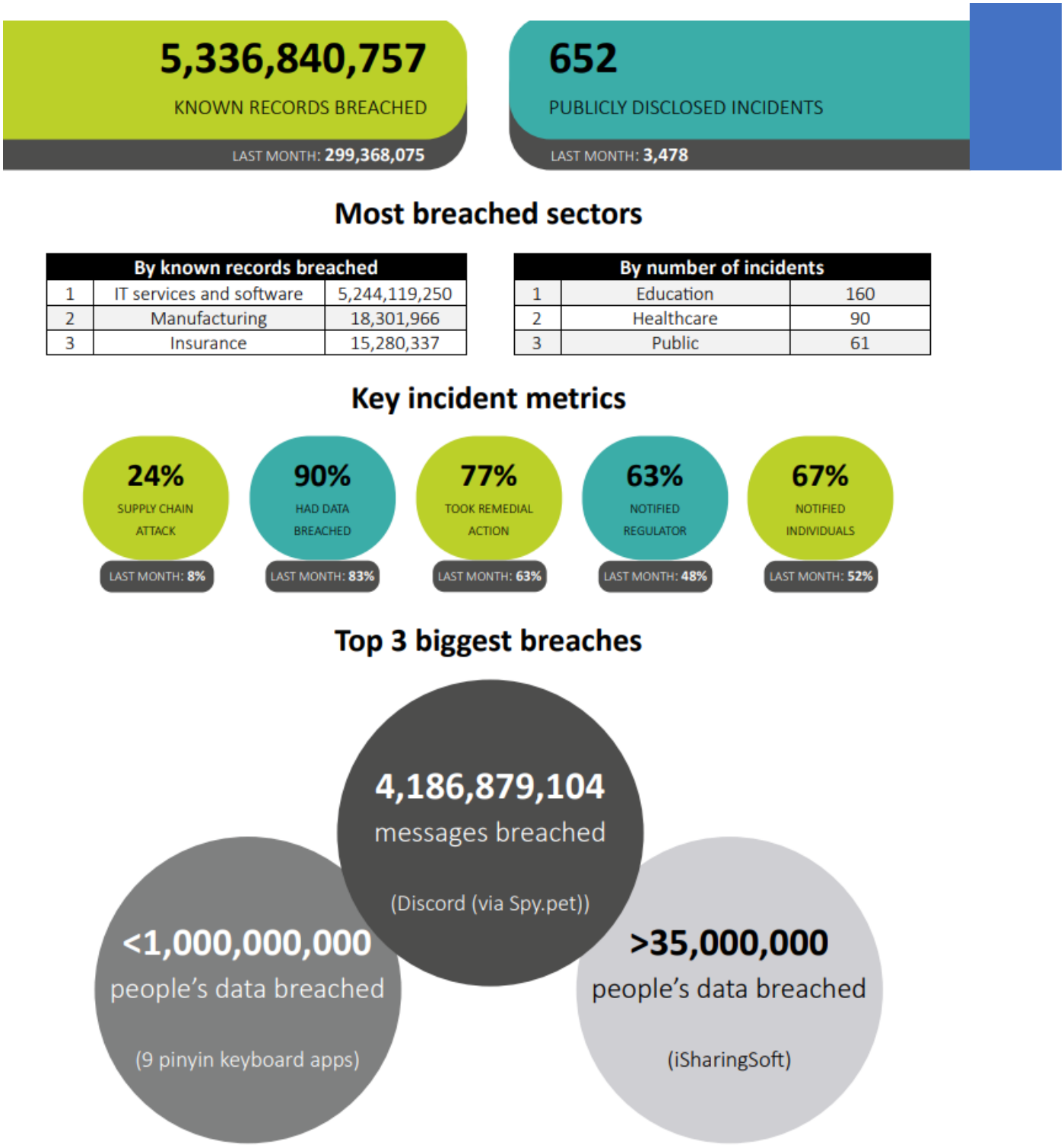


FIGURE 1 IT GOVERNANCE 2024

Baseline Analysis and Plan

GIN AND JUICE SHOP

Table of Contents

Introduction

As more companies and organisation go fully digital, they are increasingly vulnerable to cyber threats. The National Cyber Security Centre reports that the UK has faced as significant rise in cyberattacks, reporting 430 incidents up from 370 in the previous year (NCSC, 2024) These attacks have impacted critical institutions including hospitals and government agencies.

The financial repercussions of such breaches are substantial. According to IBM (2024) cost of data breach report, the global average cost of a data breach has risen to £3.87 million, an increase of 10%.

This document aims to evaluate the security situation of the Gin and Juice shop (https://ginandjuice.shop/), identify vulnerabilities and establish a base line for further assessment.

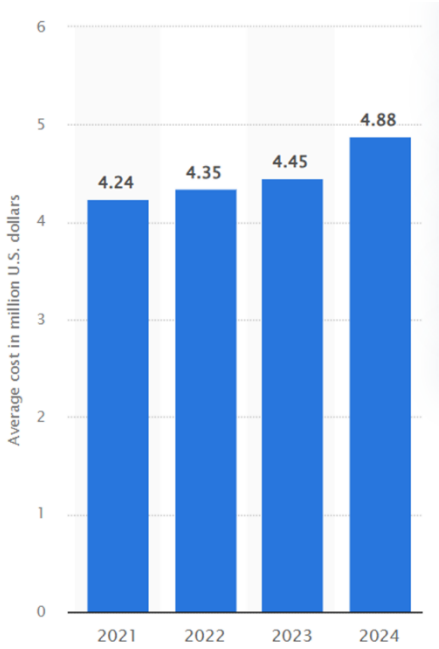


FIGURE 2 EXTRACT FROM STATISTA (2024)

Security Challenges

Generic

SQL Injection	In 2024, security researchers discovered a significant SQL injection vulnerability in a third-party website used by smaller airlines to access the TSA's Known Crewmember (KCM) system (The Verge, 2024).
Cross-Site Scripting (XSS)	In 2014, eBay suffered an XSS attack where attackers injected malicious JavaScript, tricking users into entering their credentials on phishing pages (BBC News, 2014).
Cross-Site Request Forgery (CSRF)	In 2010, a CSRF vulnerability in YouTube allowed attackers to force users into subscribing to channels without their consent (Acunetix, 2010).
Insecure Authentication	In 2012, LinkedIn was breached due to weak password hashing, exposing 117 million user passwords (The Guardian, 2016).
Security Misconfiguration	In 2018, Panera Bread exposed millions of customer records due to an insecure API endpoint left unprotected (CSO Online, 2018).
Outdated Software	The Equifax breach in 2017 was caused by an unpatched Apache Struts vulnerability, exposing 147 million records (Jason, 2019).

Specific

GDPR Compliance Risks	British Airways was fined £20 million in 2020 after failing to secure customer data, leading to the exposure of 400,000 payment details (BBC News, 2020).
Financial Transaction Security	In 2013, Target suffered a data breach that compromised 40 million credit card numbers due to poor security on its payment system (The Guardian, 2013).
API Security	In 2019, Facebook exposed 540 million user records due to a misconfigured API, leaving sensitive data publicly accessible (BBC News, 2019).
DDoS Attacks	In 2016, the Dyn DNS provider suffered a massive DDoS attack using IoT devices, taking down major websites like Twitter, Netflix, and PayPal (The Guardian, 2016).

Standards and Compliance

GDPR (General Data Protection Regulation)	Required for handling personal data of EU users.
ISO 27001	Best practices for information security management.
PCI DSS (Payment Card Industry Data Security Standard)	Required if processing credit card transactions.
OWASP Top 10	Industry standard awareness document for web security risks.
NIST Cybersecurity Framework	Provides guidelines for managing cybersecurity risk.

Tools

Tool	*Primary Use*	*Justification*	*Similar Tools*
Burp Suite	Manual and automated web application security testing.	Comprehensive and trusted tool for web app security testing. It offers manual and automated scanning with key features for interception and vulnerability analysis.	No other free tool matches Burp Suite's combination of web app-specific testing, ease of use, and comprehensive feature set. Alternatives like Wireshark focus on network analysis, not web app vulnerabilities.
OWASP ZAP	Vulnerability scanning and security analysis for web apps.	Free and open source with a user-friendly interface. Active and passive scanning, spidering, fuzzing, and more for comprehensive scanning.	Commercial tools like Acunetix and Nessus offer more advanced features but are paid. ZAP provides a similar level of automation and manual testing for free.
Nmap	Network scanning for open ports and vulnerabilities in services.	Widely used and trusted for network mapping and service detection. It's quick, flexible, and offers various scanning options for network vulnerability testing.	Alternatives like Nessus and Zenmap offer more advanced functionality, but Nmap is sufficient for basic scanning and network reconnaissance at no cost.
NSLookup	DNS queries to gather domain, subdomain, and IP address information.	Simple, fast, and effective for DNS resolution. Provides basic info about the target domain.	nslookup is better for quick and simple DNS lookups because it is built-in and easy to use, whereas dig provides more detail but is not pre-installed.
Traceroute	Discovering the network path and identifying intermediate network hops.	Simple tool for discovering the network route and highlighting network bottlenecks, misconfigurations, or vulnerabilities.	Alternatives like PathPing and PingPlotter provide more advanced features but Traceroute is effective and easy to use for basic network path discovery.
SSL Labs	SSL/TLS configuration testing and assessment.	SSL Labs provides a detailed analysis of a website's SSL/TLS configuration, including encryption strength and security issues.	SSL Labs provides one of the most comprehensive and detailed reports available.

Potential Impact on Normal Operations

- Scanning tools may generate additional traffic and impact website performance.
- Automated testing should be scheduled outside peak business hours.
- Penetration testing should be done in coordination with IT teams to prevent service disruption.

Methodology

Remote	Local
Penetration Testing	Penetration testing
Compliance Assessment	Endpoint Security
Vulnerability Scanning	Wi-Fi Security
Social Engineering	Physical Security

Manual Manual assessments involve human involvement, expertise, and decision-making to identify vulnerabilities, as opposed to relying solely on automated tools.
Automated Automated assessments rely on pre-configured tools or scripts to identify vulnerabilities and security weaknesses without human intervention during the scan process.

Since the Gin and Juice Shop is a test website with no internal access or staff the, primary approach will be remote testing. Automated tools will be used for quick vulnerability scans while manual testing will help identify complex issues such as logic flaws or other vulnerabilities that automated tools may miss.

Remote Testing

Vulnerability Scanning

- Identify publicly accessible vulnerabilities on the website
- Burp Suite, OWASP ZAP
- Automated scanning of the site's infrastructure to detect known vulnerabilities.

Penetration Testing

- Simulate external attacks on the website to assess its security posture and determine if vulnerabilities can be exploited by an attacker.
- Burp Suite, OWASP ZAP
- Manual penetration testing focusing on web application vulnerabilities.

Compliance Assessment

- Ensure the site adheres to basic security best practices, such as using proper SSL/TLS configurations, secure HTTP headers
- SSL Labs
- Running automated checks for compliance with security standards.

Assumptions and Limitations

Assumption

Test Website Availability: It is assumed that the Gin and Juice Shop test website will remain accessible during the testing process without interruptions. Any downtime could affect the accuracy of the assessment.

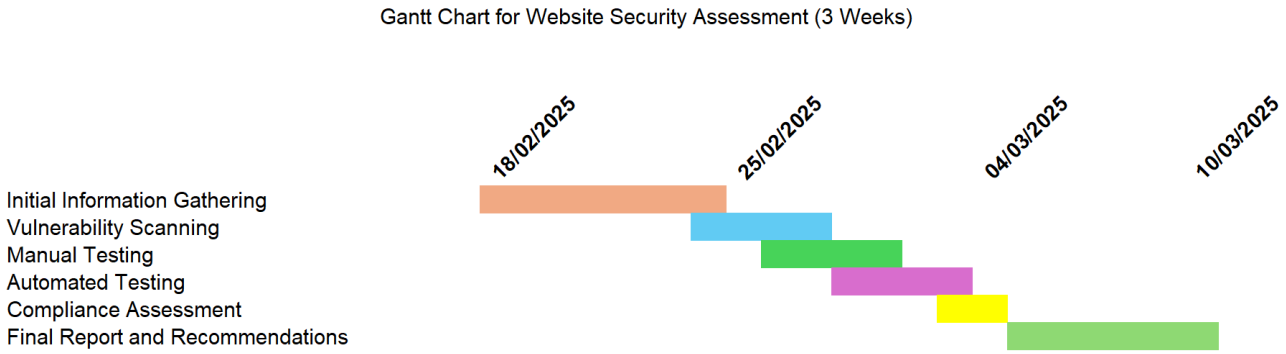
No Internal Access: It is assumed that the website has no internal systems or staff that can provide further insight or support during testing. All testing will be conducted remotely based on publicly available information.

Limitations

Limited to External Assessment: The assessment is restricted to the website's public facing assets, such as the domain, external interfaces, and web application. Internal network vulnerabilities, physical security weaknesses, or endpoint security will not be assessed.

No Staff Interaction: With no staff or support, it will not be possible to test for social engineering or assess potential security risks associated with human interaction, such as phishing susceptibility.

Timeline



Summary

Key Observations

Generic Risks: Potential vulnerabilities such as SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) and insecure authentication practices may expose the website to exploitation.

Specific Risks: GDPR compliance risks, financial transaction security, API vulnerabilities, and susceptibility to Distributed Denial of Service (DDoS) attacks may pose threats to the business operations and reputation.

Compliance Gaps: Risks of non-compliance with key industry standards like GDPR, ISO 27001 and PCI DSS could result in significant legal and financial consequences.

Next Steps

The next phase of this assessment will involve conducting a detailed security scan using tools such as Nmap, OWASP ZAP and Burp Suite.

Refences

Acunetix (2010) *Dangerous XSS vulnerability found on YouTube – the vulnerability explained*. Available at: https://www.acunetix.com/blog/articles/dangerous-xss-vulnerability-found-on-youtube-the-vulnerability-explained/ (Accessed: 16 February 2025).

BBC News (2014) *JP Morgan hack hits 76 million households*. Available at: https://www.bbc.co.uk/news/technology-29241563 (Accessed: 16 February 2025).

BBC News (2019) *Facebook stored hundreds of millions of passwords in plain text*. Available at: https://www.bbc.co.uk/news/technology-47812470 (Accessed: 16 February 2025).

BBC News (2020) *EasyJet hack: Nine million customers' details accessed*. Available at: https://www.bbc.co.uk/news/technology-54568784 (Accessed: 16 February 2025).

CSO Online (2018) *Panera Bread blew off breach report for 8 months, leaked millions of customer records*. Available at: https://www.csoonline.com/article/565050/panera-bread-blew-off-breach-report-for-8-months-leaked-millions-of-customer-records.html (Accessed: 16 February 2025).

IBM (2024) *Cost of a data breach report 2024*. Available at: https://www.ibm.com/reports/data-breach (Accessed: 16 February 2025).

IT Governance (2024) *Global data breaches and cyber attacks in January 2024: 295,308,29012 records breached*. Available at: https://www.itgovernance.co.uk/blog/global-data-breaches-and-cyber-attacks-in-january-2024-29530829012-records-breached (Accessed: 16 February 2025).

National Cyber Security Centre (NCSC) (2024) *NCSC Annual Review 2024*. Available at: https://www.ncsc.gov.uk/files/NCSC_Annual_Review_2024.pdf (Accessed: 16 February 2025).

Statista (2024) *Global average cost of a data breach 2024*. Available at: https://www.statista.com/statistics/987474/global-average-cost-data-breach/ (Accessed: 16 February 2025).

The Guardian (2013) *Target data breach affects 40 million credit and debit card accounts*. Available at: https://www.theguardian.com/business/2013/dec/19/target-breach-credit-card-accounts (Accessed: 16 February 2025).

The Guardian (2016) *DDoS attack that disrupted internet was largest of its kind in history, experts say*. Available at: https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet (Accessed: 16 February 2025).

The Verge (2024) *Airline security bug exposed TSA security database to hackers*. Available at: https://www.theverge.com/2024/9/8/24239026/airline-security-bug-tsa-security-database-sql-injection-hack (Accessed: 16 February 2025).

Thomas, J. (2019) *A case study analysis of the Equifax data breach*. Available at: https://doi.org/10.13140/RG.2.2.16468.76161 (Accessed: 16 February 2025).