McGill | School of Continuing Studies

Risk Assessment

Celia Fuentes

CCCS 453 – Security Risk Management and Governance

Table of Contents

Introduction

The following is a revised version of a Risk Assessment Project I did for the Security Risk Management and Governance course in the Certificate in Applied Cybersecurity at McGill's School of Continuing Studies.

The scenario given in this assignment describes a high-risk organization with a low-maturity security posture. It concerns a start-up company, Financial Info Quest (FIQ), whose service is to provide fast, up-to-date financial news and data to their clients that are investment companies.

Students were asked to find five risks, and for each include:

- A Brief Description
- A Threat Source
- A Worse-Case Threat Event
- A Vulnerability being exploited
- Describe the Threat Impact
- An Assessment of Risk based on research and citations
- Mitigations Recommendations

The risks I identified are in the order that they appear in the scenario. Students were free to make assumptions to flesh out the scenario further, provided they were explicitly stated. I put my assumptions for each risk in its "Brief Description" sub-section.

Risk #1: Sign in without Multi-Factor Authentication (MFA)

Brief Description: Members can access the private section of the website with a password. I assume the password requirements are weak and that there is no additional form of authentication.

Threat Source: In the threat event below, a hacker exploits the vulnerability of a member with a non-secure password to access their FIQ account.

Worse-Case Threat Event: A member's (company) confidential information is breached on the FIQ platform due to poor authentication processes. The impersonator goes on to sell the data on the dark web. The company sues FIQ because it argues that the authentication processes should have been stronger. FIQ's reputation drops, and it must pay an expensive settlement.

Vulnerability Exploited

1. No protection against the misuse of stolen credentials

High Adverse Impact: In 2021, the average cost of credential theft for an organization was $4,37 billion[i]. Costs include non-PCI-DSS compliant authentication related fines, increased fees, potential lawsuits settlements due to authentication liability and a hit to business reputation.

Assessment of Risk
High Likelihood[ii]: 80% of security incidents are caused by stolen passwords and 17% of incidents involved guessed password; since 2017, 555 million stolen passwords are available on the dark web; 62% of workers share passwords in plaintext by SMS and email messages. An additional form of authentication is essential.[iii]
High Impact Likelihood: There have been several examples of lawsuits due to poor security measures, including lack of MFA.[iv] Compromised credentials are the leading cause of data breaches[v].

Mitigation Recommendations

1. Educate members on best practices for keeping passwords secure,[vi] for example not sharing passwords
2. Since member accounts may include partial information on payment details, follow PCI-DSS password requirements: minimum complexity of 8-12 alphanumeric characters[vii]; to be changed at least every 90 days[viii]
3. MFA can block up to 99% of attacks[ix]; enabling MFA is an efficient additional way to authenticate users signing into the FIQ website

Risk #2: Outdated, Unpatched and Misconfigured Platform

Brief Description: The student-made platform is installed on Windows servers with the back end using Oracle database. I assume that the students chose outdated Oracle Database version 12.1.0.2 (12c released in July 2013[x]) and Windows 10 because those were the versions they used at their university.

Threat Source: A criminal group exploiting a structural vulnerability due to poor infrastructure decisions.

Worse-Case Threat Event: a group with medium technical capabilities is able to target outdated, unpatched and misconfigured software and systems; their motivation is financial and they access the FIQ Oracle database server; stealthily gain privileged access to the OS and infect Windows with ransomware (ex. WannaCry) that uses command and control to encrypt critical files and systems; they demand an amount that FIQ is unable to pay; the company is unable to recover the data by other means; FIQ/client data is sold on the dark web.

Vulnerability Exploited

1. CVE-2015-4888[xi] and CVE-2015-4796[xii] vulnerabilities in Oracle database that allow unauthorized remote access to authenticated users
2. CVE-2017-0144[xiii] vulnerability in Windows that allows remote attackers to execute arbitrary code

High Adverse Impact: all five impact types are affected. Harm to operations (cannot do business nor access critical systems); harm to assets (loss of information systems); harm to individuals (loss of customer PII); harm to other organizations (relational harm to customers); harm to the nation (100 investment boutiques that could in turn have clients throughout the country). The outcome would be the total loss of critical data and shutdown of FIQ.[xiv]

Assessment of Risk

High Likelihood: Around 85% of security breaches are due to unpatched software because it is easier to exploit known issues than to find zero-day vulnerabilities.[xv] WannaCry attacks increased 58% from January to March 2021.[xvi] It continues to be a top threat because of unpatched system or reworked versions that don't have an embedded kill switch.[xvii]

High Likelihood of Impact: Furthermore, ransomware payments increased 311% to $350 million.[xviii] The impacts are often so severe that 25% of small businesses file for bankruptcy and 10% go out of business after just one breach.[xix]

Mitigation Recommendations

1. Immediately perform the Oracle and Windows patches;
2. Assess the cost-benefit of effective patch software management for all FIQ systems[xx]
3. Assess the cost-benefit of data backups to enable data recovery[xxi]

Risk #3: Physical access security

Brief Description: The servers are in a private room, in a downtown office building with a high vacancy rate. I assume the private room has no lock or alarm in a building with no security to control access.

Threat Source: Criminal group that exploits a human-made environmental vulnerability due to a lack of basic physical deterrence to theft, destruction or manipulation of critical on-site assets.

Worse-Case Threat Event: With 100 boutiques in Montreal and Toronto interested in FIQ's services, the word has spread that it could quickly become a market disrupter. A criminal gang breaks into the FIQ offices to install keylogging and webcam monitoring. Even before the startup really begins to do business, external adversaries have already gained access with stolen credentials and are monitoring all strategic, hiring, security, business and operational decisions and processes remotely.

Vulnerability Exploited

1. No meaningful physical deterrence

High Adverse Impact: Damage or theft of assets (devices, documents), vandalism, employees no longer feeling safe.[xxii] The loss of certain data may be irreplaceable.

Assessment of Risk
High Likelihood: The physical sphere is very much part of the threat landscape. Around 85% of cybersecurity breaches had a human element which included insider threats and physical breaches.[xxiii]
High Likelihood of Impact: While the cost of replacing lost/stolen equipment and cleaning up vandalism may not be dramatically high, the loss of data could be irreplaceable.

Mitigation Recommendations[xxiv]

1. Daytime physical deterrence: magnetic cards for general staff to enter main company space and additional keycode pads to enter restricted areas that can only be accessed by limited personnel
2. Additional off-hour physical deterrence: install strong locks, alarms, motion detectors, window bars
3. Offsite backups in case of theft, vandalism or natural disaster
4. Educate staff to never leave devices unattended, to not allow tailgating (letting unknown/unauthorized persons into office space), and to follow a clear desk policy[xxv]
5. Enable MFA to mitigate against the use of stolen credentials
6. Logs to monitor on-site and remote access to devices

Risk #4: Inadequate Access Control

Brief Description: Every employee can access any FIQ resource on-site or from a remote location. I've made the additional assumption that there is no resource or log monitoring.

Threat Source: A hacker exploits organizational-wide excessive access because it facilitates the abuse of access rights for financial gain.

Worse-Case Threat Event: a well-intentioned employee falls for an email phishing scam and clicks open a file that installs keylogging malware. Since the employee has access to all FIQ resources, more malware can easily spread throughout all systems over several days[xxvi]. The hacker sets up privileged access remotely for themselves and installs backdoors throughout the network to make exfiltration of files possible at any moment. FIQ is not even aware of the intrusion with the hacker currently hidden and using FIQ servers to mine for cryptocurrency[xxvii].

Vulnerability Exploited

1. Organizational-wide lax access control to all resources
2. No audit trail or resource monitoring

High Adverse Impact: the threat event results in the misuse of FIQ resources but could also lead to accidental harm to the integrity or availability of data by employee modification or deletion of files.

Assessment of Risk

High Likelihood: 82% of breaches are due to human error[xxviii]. Granting excessive rights to all employees increases the speed and magnitude of the resulting impact since there are no controls to block access to critical systems and sensitive data. In 2018, cryptojacking increased by 450%[xxix].

High Likelihood of Impact: Cryptojacking will have a direct impact on FIQ's core mission to provide fast, up-to-date financial data and news to clients because resources are diverted to crypto mining. A noticeable decrease in device productivity, shutdown due to insufficient processing power, battery, fan and maintenance related costs, as well as increased electricity bills will all adversely affect FIQ's bottom line[xxx]. Clients will eventually switch to a provider that can provide news faster.

Mitigation Recommendations

1. Grant access based on the least privilege principle for both on-site and remote access
2. Develop an Information Security Management System (ISMS) to define organizational baseline of systems and assets, to clearly define roles and responsibilities, and to enforce the notion of accountability with log monitoring
3. Use browser extensions to block coin mining[xxxi]
4. Assess the cost-benefit of systematically monitoring device resources (electricity, RAM, battery)[xxxii]

Risk #5: Rushed Software to Manage Payments

Brief Description: FIQ hires students to develop software to manage payments automatically. The key assumption I make revolves around weak encryption during transit.

Threat Source: Criminal groups actively try to acquire payment information by exploiting vulnerability in weak encryption. Non-tested encryption will fail to protect the confidentiality and integrity of payment data against criminal groups[xxxiii]

Worse-Case Threat Event:
An adversarial external threat actor can view payment data at end points and while in transit. They copy and keep the data to sell to the highest bidder.

Vulnerabilities Exploited[xxxiv]

1. Weak encryption: FIQ is not using the industry-tested AES, which is considered PCI-DSS compliant that fulfills Requirement 4.1 concerning encryption[xxxv]
2. Lax control access measures that don't follow Requirement 7.2 to restrict access to payment data based on role and responsibilities[xxxvi]

High Adverse Impact: weak encryption violates PCI-DSS compliance, compromises the confidentiality of payment information, and results in fines and lawsuits.

Assessment of Risk
High Likelihood: it is forecasted that losses from mostly online fraudulent transactions will reach $165.1 billion over the next 10 years[xxxvii].
High Impact likelihood: non-compliance leads to investigation fees, heavy fines and fees, and FIQ could also face lawsuits[xxxviii].

Mitigation Recommendations

1. I strongly advise against using in-house tools for payment systems because of the complexity, the high liability, maintenance and compliance costs will quickly surpass any savings from avoiding payment fees. Use a third-party vault service that is PCI compliant. Although there are fees, they are a good fit for fast-growing businesses. They will handle PCI DSS compliance and payment data storage externally.[xxxix]
2. If the first mitigation is not implemented: test for weak encryption of payment and other systems[xl]
3. Isolate payment systems from other segments of the network
4. Implement access control to all payment files and systems to need-to-know

Endnotes

Risk #1: Sign in without Multi-Factor Authentication (MFA)

[i] https://www.beyondidentity.com/blog/cost-passwords

[ii] https://financesonline.com/password-statistics/

[iii] https://www.cyber.gc.ca/en/guidance/best-practices-passphrases-and-passwords-itsap30032

[iv] https://www.cybertalk.org/2022/11/02/4-data-breaches-in-3-years-now-an-ftc-lawsuit/

[v] https://www.keepersecurity.com/blog/2021/08/11/data-breach-costs-are-at-record-highs-and-most-are-caused-by-stolen-login-credentials/

[vi] *Ibid.*

[vii] PCI-DSS-v4_o.pdf, Strong Authentication, sub-requirement 8.3.6, p.174 available at https://www.pcisecuritystandards.org/document_library/

[viii] PCI-DSS-v4_o.pdf, Strong Authentication, sub-requirement 8.3.9, p.177 available at https://www.pcisecuritystandards.org/document_library/

[ix] https://financesonline.com/password-statistics/

Risk #2: Outdated, Unpatched and Misconfigured Platform

[x] https://en.wikipedia.org/wiki/Oracle_Database#cite_note-17

[xi] CVE-2015-4888, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4888

[xii] CVE-2015-4796, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4796

[xiii] https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2017-0144

[xiv] https://blog.purestorage.com/perspectives/whats-the-worst-case-scenario-for-a-ransomware-attack/

[xv] https://www.mainstream-tech.com/unpatched-vulnerabilities/#:~:text=The%20Department%20of%20Homeland%20Security,security%20breaches%20involve%20unpatched%20software.

[xvi] https://securityintelligence.com/articles/what-has-changed-since-wannacry-ransomware-attack/

[xvii] https://www.csoonline.com/article/3660575/wannacry-5-years-on-still-a-top-threat.html

[xviii] https://www.spiceworks.com/it-security/cyber-risk-management/articles/ransomware-payment-to-pay-not-to-pay/#:~:text=Despite%20federal%20and%20homeland%20security,still%20unable%20to%20recover%20data.

[xix] https://financesonline.com/cybercrime-trends/

[xx] https://www.mainstream-tech.com/unpatched-vulnerabilities/#:~:text=The%20Department%20of%20Homeland%20Security,security%20breaches%20involve%20unpatched%20software.

[xxi] Data encrypted for impact: https://attack.mitre.org/techniques/T1486/

Risk #3: Physical access security

[xxii] https://alarmtech.ca/2020/11/03/commercial-robbery-vs-commercial-break-ins/

[xxiii] https://www.deloitte.com/global/en/services/risk-advisory/blogs/physical-security-the-shift-in-perspective.html#endnotes

[xxiv] https://www.tutorialspoint.com/what-is-physical-security-in-information-security

[xxv] https://blog.usecure.io/physical-security-risks

Risk #4: Inadequate Access Control

[xxvi] https://www.passportalmsp.com/blog/top-3-risks-of-not-having-a-privileged-access-management-system

[xxvii] https://financesonline.com/cybercrime-trends/

[xxviii] https://www.grcelearning.com/blog/human-error-is-responsible-for-85-of-data-breaches

[xxix] https://financesonline.com/cybercrime-trends/

[xxx] https://www.interpol.int/en/Crimes/Cybercrime/Cryptojacking

[xxxi] https://www.acronis.com/en-us/blog/posts/how-to-block-cryptomining-scripts-in-your-browser/

[xxxii] https://www.interpol.int/en/Crimes/Cybercrime/Cryptojacking

Risk #5: Rushed Software to Manage Payments

[xxxiii] https://en.wikipedia.org/wiki/Bruce_Schneier#Cryptography

[xxxiv] https://www.pcidssguide.com/what-are-the-pci-dss-encryption-requirements/

[xxxv] PCI-DSS-v4_o.pdf, Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and documented, 4.2.1, p.102 available at https://www.pcisecuritystandards.org/document_library/

[xxxvi] PCI-DSS-v4_o.pdf, Access to system components and data is appropriately defined and assigned, sub-requirement 7.2.2 p.154 available at https://www.pcisecuritystandards.org/document_library/

[xxxvii] https://www.bankrate.com/finance/credit-cards/protect-your-data-with-new-secure-payment-methods/#:~:text=By%20and%20large%2C%20credit%20cards,accounts%20and%20personal%20information%20safe.

[xxxviii] https://onlinects.com/2020/05/31/consequences-of-not-being-pci-compliant/#:~:text=You%20could%20end%20up%20paying,could%20not%20settle%20the%20fines.

[xxxix] https://www.pcidssguide.com/advantages-of-using-a-credit-card-vault-for-pci/

[xl] https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/09-Testing_for_Weak_Cryptography/04-Testing_for_Weak_Encryption