# *6204*
# *Information Security*

## *Assignment 1*

# *Security Report on Intuit*

## 1.0 Introduction:

### 1.1Purpose:

The risk assessment report was created to identify threats, vulnerabilities that are present in an organization, furthermore, discuss impact and capabilities these attacks can have on an organization. The report was created on the company Intuit Inc., an enterprise software and a high-tech company, whose primary domain is finance. Furthermore, the report helps to provide risk mitigation mechanisms and countermeasure to nullify the attack.

### 1.2Basic company information:

Intuit is a global technology platform that helps their customers and communities overcome their most important financial challenges, through their products and services. It's in the enterprise software industry. Intuit is a public company and the company's headquarters is located in Mountain view, California. Integrity without compromise is one of the core values that the company holds, it further expands on courage, ethnic diversity, gender representation and pay equity.

### 1.3 Company History:

Intuit was founded by Scott Cook and Tom Proulx in 1983, Palo Alto, California. According to Intuit the company was an "idea that turned into a reality". When Scott Cook and his wife were paying their bills, he felt the need of an automated system that could mitigate the hassle of paying bills. This particular incident has inspired him to create Intuit. The company emphasizes on work life balance and offers support in mental health, medical and dental benefits, moreover, bolstering the work community with training events, internal workshops to encourage knowledge sharing.

## 1.4 Mission Statement:

We are a purpose- driven, values-driven company. Our mission to empower prosperity around the world is why we show up to work every single day to do incredible things for customer. Our values guide us and define what we stand for company.

## 1.5 Product/Service and customer:

Intuit Inc. provides financial management, compliance products and services for consumers, small businesses, self-employed, and accounting professionals in the United States, Canada, and internationally. Intuit, at core, product focused company also known as "house of brands". Moreover, it's a financial focused domain. Some of its brands are Turbo Tax (a tax preparation app), Mint (personalized finance app).

## 1.6 Future business :

Intuit is building a strategy to be an AI driven plat-form, their aim is to solve customer's woes and deliver impeccable services to them. Their strategy involves a five- step plan called "Big Bets". The first talks about on how application of AI can revolutionize the speed of benefits provided to the customer. The second and third step involves connecting experts to customers to cater their needs, through virtual platforms with AI, and they are developing a virtual financial assistant to tackle monetary problems by helping them find the right product, respectively. Lastly, the last two points focus on how they are planning to be the center of small-scale businesses.

## 2.0 Risk Assessment:

Risk Assessment critically analysis risks present in any organization, primarily in this report were discussing in a technical atmosphere. This assessment assists in giving us a perspective on how, plethora of threats are faced on a regular basis in the IT world. Furthermore, it aids in understanding the degree and the nature of threat, it provides countermeasures and mitigation methods to increase the scale of protection. Any system in an organization requires constant updates supporting its business, so that it can avoid potential new risks. Performing a risk assessment helps in identifying different vectors of threats.

## 2.1 Constituent elements present in Threat and Risk Assessment:

### Threat:

When an institution or an organization is under an attack, a threat assessment provides a review of the capacity of the attack, it also addresses the vulnerability present in the network. Moreover, it deals with sensitive information while creating a report, primarily identifying the threat type and source of attack.

### Vulnerability:

Vulnerabilities are the shortcomings present in the network a of system, to quantify a threat it is assigned with risk rating. Moreover, by analyzing the level of the threat, it provides countermeasure to mitigates the risks and restore the system's security level.

### Asset:

A technological organization possess a data that it has acquired from its client, and the data is the biggest asset it has under possession and holds a value. It is often an asset because it contains confidential information. Moreover, employees, infrastructure, support systems are also an asset.

## 2.2 Organization’s user and technology details:

Intuit collects and stores humongous amounts of data, these data ate highly sensitive and classified. It offers service through one of its products called TurboTax, which is a software where 17.5million of Americans use to file their income tax returns. Intuit boasts of about 50 million customers, of which, about 35million of them use either Turbo tax and Quick books. Quick book is another intuit product, which provides accounting services. More than 12 million employees and 1.5 million small businesses are accounted for or paid through its software.

| Intuit Products | Details of Product |
|---|---|
| Turbo tax | Software package for preparation of American income tax returns |
| Quick books | Accounting software package, accept business payments, manage and pay bills and payroll functions |
| Mint | Personal financial management website and mobile app |

| Intuit Products | Users of Products | Data Collected |
|---|---|---|
| Turbo Tax | American tax payers | Social security numbers<br>Previous tax returns<br>Date of birth<br>Bank and routing number<br>Business income |
| Quick books | Small and medium scale business for accounting purpose | Address<br>Tax information<br>Phone number<br>Fax number |
| Mint | Bill payment service used by most organization and individuals and also budget tracking and planning. | Bank details<br>Credit card type<br>Verification code<br>Transaction reference<br>Card expiry date |

## Intuit tech details

| Intuit Products | Database | Operating system | Networks |
|---|---|---|---|
| Quick books | Oracle<br>My SQL<br>Microsoft SQL | Microsoft<br>Windows<br>Mac os | Windows firewall |
| Turbo tax | My SQL | Windows<br>Macintosh<br>Android<br>IOS | Windows firewall |
| Mint | MY SQL | Windows<br>IOS | Windows firewall |

## 2.3 Identification of threats:

| Origin of threat | Threat Kind |
|---|---|
| 1. Nature | • Earthquakes<br>• Floods<br>• tsunamis |
| 2. Human negligence | • Downloading codes without integrity<br>• Unauthorized system access |
| 3. Hackers | • Injecting malicious code<br>• Stealing login details<br>• Traffic interception<br>• Web defacement |

## 2.4 Calculation of risk impact:

### Risk model:

**Risk = Impact * Threat Likelihood**

### Impact:

| Impact | Details of Impact |
|---|---|
| High (100) | The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. |
| Medium (50) | The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. |
| Low (10) | The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. |

## Threat Likelihood:

| Likelihood | Details of Likelihood |
|---|---|
| High (1.0) | Vulnerability affects a majority of system components. Exploitation significantly increases the probability of additional vulnerabilities being exploited |
| Medium (0.5) | Vulnerability can be expected to affect more than one system element or component.<br>Exploitation increases the probability of additional vulnerabilities being exploited. |
| Low (0.1) | Effects of vulnerability tightly contained. Does not increase the probability of additional vulnerabilities being exploited**.** |

## Threat Likelihood:

According to the risk model, risk is the probability of the threat occurrence and the impact or the influence the threat can make. Likelihood measures the chances or reoccurrence of threat on a system. Post measuring the frequency of threat, the risk model helps in identifying the capacity of the threat, and suitable countermeasures are applied to nullify the attack.

## Impact:

Impact addresses and quantifies the total damage an attack has rendered on a system of an organization or an individual. A cyberattack can damage the infrastructure, accountability, reputation of the organization and incur huge monetary loses. Impact, like likelihood, through the risk model helps to identify the threat and provide mitigation methods required.

## Risk calculations:

| | | **Threat Likelihood** | |
|---|---|---|---|
| **Impact** | **Low (0.1)** | **Medium (0.5)** | **High (1.0)** |
| **Low (10)** | Low risk<br>(10*0.1) = 1 | Low risk<br>(10*0.5) =5 | **Low risk**<br>**(10*1.0) =10** |
| **Medium (50)** | Low risk<br>(50*0.1) = 5 | Medium risk<br>(50*0.5) = 25 | **Medium risk**<br>**(50*1.0) =50** |
| **High (100)** | Low risk<br>(100*0.1) =10 | **Medium risk**<br>**(100*0.5) = 50** | **High risk**<br>**(100*1.0) = 100** |

Risk scale:<br>
High -(50-100)<br>
Medium -( 10-49)<br>
Low. -(0-9)

## 3.0 Vulnerability Assessment:

After a conducting a thorough risk analysis, these were the following vulnerabilities identified in the organization Intuit. Inc.

| Vulnerability | Details | Origin of Threat |
|---|---|---|
| 1. Weak passwords | The password created by the organization is weakly constructed and not strong enough to protect from threats. | Hackers, cybercrime criminals |
| 2. Buffer overflow | There is excess data in the buffer more than which it has capacity, the attackers sent the data to be stored in the adjacent memory space | Hackers, cybercrime criminals |
| 3. SQL injection | The hacker was able to disrupt the queries in the database and view the data that is generally not permissible. They can attack the backend component. | Hackers, cybercrime criminals |
| 4. Missing data encryption | Highly sensitive data is not properly encrypted, which enables hackers to access that data, where accountability, integrity of the data is lost. | Poorly trained and irresponsible employees |
| 5. Cross site scripting | Hackers insert malicious scripts into safe and secure working networks and can carry an attack to the end user's session | Hackers, cybercrime criminals |
| 6. Download of codes without integrity checks. | The code is downloaded from an unknown source, and proper integrity checks have not taken place, without verifying its origin | Poorly trained and irresponsible employees |
| 7. Natural disaster | The organization does not have proper guidelines in order to respond and recover from any event that is caused due to natural reasons | Poorly trained and irresponsibility of organization. |

## 4.0 Risk Analysis and Management:

| S.no | Vulnerability | Threat source | Present security | Likelihood Rating | Impact Rating | Risk Rating | Mitigation methods |
|---|---|---|---|---|---|---|---|
| 1 | Weak password, Passwords can be easily guessed | Hackers, cybercrime criminals | Consist of 8 characters, of at least two numbers and two alphabets | Medium (0.5) | Medium (50) | Medium risk (25) | At least one special character and one uppercase and one lowercase character |
| **2** | Buffer overflow, data corruption in the adjacent memory space | Hackers, cybercrime criminals | N/A | Medium (0.5) | Medium (50) | Medium risk (25) | Writing secure code,<br>Use compiler warnings, use scanning applications |
| **3.** | SQL Injection, disruption of queries | Hackers, cybercrime criminals | Vulnerability scanners, firewalls | High (1.0) | Medium (50) | High risk (50) | Use prepared statements, patch and harden database |
| **4.** | Missing data encryption, poor encryption of data and loses accountability | Poorly trained and irresponsible employees | N/A | Low (0.1) | Medium (50) | Low risk (5) | Encrypt in layers, store encryption key securely. |
| **5.** | Cross site Scripting, insert malicious script | Hackers, cybercrime criminals | Windows firewall | High (1.0) | Medium (50) | High Risk (50) | Web application firewall must be used, Secure cookies, and strings. |

|  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|
| **6.** | Download of codes without integrity | Poorly trained and irresponsible employees | Training for employees | Medium (0.5) | Medium (50) | Medium risk (25) | Proper professional training required for employees |
| **7.** | Natural Disaster, caused due to environment | Poorly trained workers and irresponsibility of organization. | Week guidelines and policies | Medium (0.5) | High (100) | High Risk (50) | Employees must be professionally training. Infrastructure should be disaster proof. |

## 5.0 Summary of report:

A risk analysis has been performed on the organization Intuit Inc, headquarters located in Mountain View, California. The enterprise software industry is primarily a product -based company, in this report, risk analysis has been done on the products Quick books, Turbo Tax, and Intuit Mint.
The source of the threat and threat kind have been identified, and vulnerabilities have been identified. After applying the risk model, the level of risk for each kind of attack has been assigned. Lastly, based on the degree and the impact of the attack, mitigation methods have been provided.