Risk Assessment for Old People Help Website (patent pending)

By Ethan Frost

**Background**

We are creating a website with the purpose of assisting the elderly and their carers, by providing them with a connection to a carer over the website who can provide health support, legal support, as well as being on standby for any emergencies, through an SMS built into the web page. Whilst using the website, the elderly people would be providing sensitive information such as medical conditions, age, home address and race, all of which would be lucrative to a threat actor.

**Assets**

The most valuable asset to the support website in this situation is the data of the users, which includes both the elderly and their carers using it for support. Ensuring the data is compliant with the CIA Triad should be the top priority of the website (this entails that the data must be confidential, have integrity, and be available whenever needed), as if a data breach was to occur and user data was to be unintentionally accessed, it would lead to many negatives for its users through data being sold. In addition, the website itself would be negatively affected, as it is likely to have fewer users due to a loss of trust over such an incident.

A crucial asset to our development would be the database. This asset ties into the user data, as if a threat actor gained complete access to the database, then all of the user data could be collected to sell on or destroyed. As such, encrypting communications between the database and users of the website is essential to keep user data secure.

One final asset of importance would be the devices of the software developers that are utilised in the creation of the website. If a threat actor was to physically steal a device used in the creation of the website, then it could be used to alter the website to cause negative impact in the future or lead to a data breach. In addition to this, if a backup is not created of the website then it could take a long time to bring the website back into its intended state, meaning a prolonged period of time where business as usual cannot take place.

**Vulnerabilities**

A potential vulnerability with the website would be a lack of encryption. Without specific use of encryption in the code of the website, a threat actor could easily listen into the data being transferred between the website and the database. If the website lacks basic encryption, it would be all too easy for a threat actor to gain access and begin to exploit it, which is likely to lead to a data breach.

Another vulnerability with the website would be the target users. This is because elderly people are often the targets of cyber attacks, such as Phishing, due to their unfamiliarity with the technology or more trusting nature. These weaknesses can be easily exploited by threat actors to gain access to the website and cause a data breach or loss in functionality through a DDOS (sending so many requests to connect to a website that no legitimate user can connect) or similar attack.

One more vulnerability is the use of communal computers in the university during the creation of the website. If a threat actor was to come internally from the university due to personal reasons or vengeance, then a data breach could easily occur if the computer is left open and unattended.

One final vulnerability with the website would be that it is being worked on from multiple devices with both communal computers and home devices. With files being moved between computers, either via memory sticks or the cloud, they could be intercepted in the process by a threat actor. This could result in data being used to tamper with the website, or gain unintentional access to customer data.

**DREAD:** The DREAD risk model was created by Microsoft as a way to assess and rank threats in terms of risk. The acronym breaks down threats as follows: the damage they cause to assets (D), how easily can the attack be reproduced (R), how easily can an attack be performed to exploit a system (E), how many users of a network would be affected by the attack (A), and how easily the vulnerability that leads to the attack can be discovered (D). In each of these categories you give a value (in this case from 1 - 5) to represent if something is of low danger, high danger, or something in between, finally you add all of the values together for a risk to get a Risk Score, which should outline what threats need to be dealt with first. This is done to better determine the damage potential differences of threats and also represents an impact on the number of users affected.

**STRIDE**: The stride methodology was created by Microsoft to represent 6 types of common security threats. These being Spoofing: where an attacker pretends to be a legitimate user, Tampering: the modification of the system to make it illegitimate, Repudiation: Denying a certain action that is a part of a system from occurring, Information disclosure: where an attacker gains unauthorised access to confidential information (also referred to as a data breach), Denial of Service: where the attacker will prevent legitimate users from accessing the service, and Elevation of privilege: where an attacker gains higher access to a system than they are intended to, usually from a user with the higher authority. The purpose of STRIDE is to analyse vulnerabilities against each system component which could be exploited by an attacker to compromise the whole system

**Risk Tables:** In these tables I will be plotting each risk on a scale of 1 - 5, with 1 being low danger, and 5 being high danger to begin with using the DREAD risk model. After this I will be using the STRIDE model to demonstrate what types of attacks the different vulnerabilities are at risk to, and finally I will be creating a Risk Matrix to visually demonstrate how damaging vulnerabilities can be.

**DREAD table:**

| Vulnerability | Damage | Reproducibility | Exploitability | Affected Users | Discoverability | Risk Score | Treatment Priority |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Lack of Encryption | 4 | 4 | 4 | 5 | 5 | 22 | high |
| Elderly Users | 4 | 5 | 5 | 3 | 4 | 21 | high |
| Communal Computers | 5 | 2 | 2 | 3 | 1 | 13 | low |
| Multiple Devices | 3 | 1 | 3 | 2 | 3 | 12 | low |

**STRIDE table:**

| Vulnerability | Spoofing | Tampering | Repudiation | Information disclosure | Denial of service | Elevation of privilege |
| --- | --- | --- | --- | --- | --- | --- |
| Lack of Encryption |  | X | X | X | X | X |
| Elderly Users | X |  |  | X | X |  |
| Communal Computers | X | X | X | X |  |  |
| Multiple Devices |  | X |  | X |  |  |

**Risk matrix:**

|  | 1: minimal damage | 2: low damage | 3: moderate damage | 4: high damage | 5: catastrophic damage |
| --- | --- | --- | --- | --- | --- |
| 5: almost certain |  |  | Elderly Users |  |  |
| 4: likely |  |  |  | Lack of Encryption |  |
| 3: possible |  |  | Communal Computers |  |  |
| 2: unlikely |  |  | Multiple Devices |  |  |
| 1: rare |  |  |  |  |  |

**Risk treatment options**

To prevent the physical theft of devices used in the creation of the website, the developers must be careful to secure them. This can be done by locking any rooms the computers are being used in, protecting the computers with a strong password, and not allowing anyone to access these devices without explicit permission. If the devices get damaged, without files being backed up, it would lead to major setbacks and prevention of business as usual for the website; in the event of theft a data breach would be more likely to occur.

To treat the risk of a lack of encryption, the solution would be to secure the cookies and other data the users send to the database with a strong encryption format, such as AES-256 with a long random encryption key. This would prevent any threat actors eavesdropping on data transfer between users and the database which could give them access to the website and the ability to cause a data breach.

To treat the risk of multiple device use, the solution would be to use a secure cloud service such as GitHub for all file sharing. This GitHub repository of code must also be protected with a strong password to keep out any threat actors. The purpose of using cloud for file sharing is to prevent any unauthorised access to the files of the website. This is because physical file sharing through devices, such as memory sticks, have the potential to be either lost or stolen, which could lead to future data breaches or tampering.

To mitigate the risk of elderly users, the solution would be to provide basic cybersecurity training to them and their carers, reducing the risk of phishing attacks. Helping them to avoid common scamming tactics would greatly help the website to maintain customer data confidentiality and integrity, as a threat actor would find it more difficult to trick elderly users to gain access to the website through an attack.

One final risk that requires consideration is the communal computers. To treat this risk, all the devices being used at the university must be secured with strong passwords, and the devices locked down when a developer leaves their station, ensuring the password protects the device from any potential threat actors within the university. In addition, the files of the website must be saved into a location that cannot be accessed by other users of the computer on different accounts; as such, any files relating to the website in the downloads area should be deleted or moved.