Staysure.co.uk Limited Case Study

Jessica Williams

Contents

1. Case Articulation

Staysure.co.uk is a limited company which specialises in over 50s insurance & lifestyle products. They were founded in 2004 and continue to trade today providing travel insurance. Staysure.co.uk hit the headlines in 2014 due to a security breach taking place the year previous which resulted in the leak of over 100,000 credit card records (Newsdesk, 2015) and other personal details, potentially affecting over 90,000 of their customers (Information Comissioners Office, 2015).

The hackers were able to gain access to the data via a vulnerability in their JBoss application server, a vulnerability for which a patch had been released 3 years prior, in 2010, Staysure.co.uk failed to apply this patch, so in 2015, after a thorough investigation the Information Commissioners Office imposed a monetary penalty of 175,000 (one hundred and seventy-five thousand) pounds due to what they considered to be an 'unbelievable' breach of the data protection act. (Information Comissioners Office, 2015)

Highlights from the report include:

- Prior to June 2008, all payment card details were held unencrypted.
- After June 2008 only CVV numbers were left unencrypted, however hackers were able to obtain the encryption keys and decrypt the data.
- In 2012 a decision was made to delete the CVV numbers however this work was never carried out.
- By May 2012, a new external system to handle payments was implemented, however the old credit card information was still stored.

Under EU Law Staysure.co.uk would be considered a data controller, meaning they determine the purposes for and how personal data they collect is processed, to protect us, data controllers are subject to several standards and regulations. (Commission)

One of them is called the Payment Card Industry Data Security Standard (PCI DSS). The PCI standard is mandated by the card brands and was implemented to increase controls around cardholder data and limit credit card fraud. (PCI Security Standards Council, 2018)

PCI DSS outlines 6 main goals, those are:

- **Build & maintain a secure network**
  This includes maintaining a firewall configuration and specifically not using default credentials.
- **Protect Cardholder Data**
  Specifically encrypting both data at rest and the transmission of that data.
- **Maintain a Vulnerability Management Program**
  The use and regularly updating of an anti-virus software & ensuring all systems & applications can be considered secure.
- **Implement Strong Access Control Measures**
  The restriction of access to data (including physical access to servers) on a need-to-know basis
- **Regularly Monitor and Test Networks**
  Recording & monitoring all access to cardholder data and the regularly testing of all systems security.
- **Maintain an Information Security Policy**
  Create & maintain an information security policy for use by all employees, even contractors.

As a company that accepts cardholder data Staysure.co.uk are required to adhere to the PCI standard, however them choosing to store 3 digit CVV numbers directly contradicts the standard and was a contributing factor to the large fine they ended up receiving (Dutton, 2015).

The Data Protection Act 1998 is a piece of legislation there to help protect us as citizens, and it legally requires everyone responsible for handling & using personal data to follow strict rules, also known as 'data protection principles' (Government, Data Protection Act 1998, 1998) meaning they must make sure the data is:

- **Used fairly, lawfully and transparently**
  Should not be processed unless certain conditions (those set out in the act) are met.
- **Used for specified, explicit purposes**
- **Used in a way that is adequate, relevant, and limited to only what is necessary**
  The data needs to be collected for a specified purpose and the data should not be processed in any manner not related to the reason it was first collected.
- **Accurate and, where necessary, kept up to date**
- **Kept for no longer than is necessary**
- **Maintain a person's rights**
  The subject should be able to request access to the information, correct mistakes, and claim compensation in case of inaccurate or breached data.
- **Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction, or damage**
  Appropriate technical and organisational measures should be taken against any unlawful, or unauthorised processing.
- **Not transferred outside the European Union**
  No personal data should be transferred to a country outside of the EEA, unless the country ensures an adequate level of protection in relation to that data.

Not only did Staysure.co.uk not adequately protect the data that they were responsible for, but they kept it for far longer than necessary and breached the above rules, meaning under Section 55A and 55B of the Act, the ICO were able to issue a monetary penalty to Staysure.co.uk. (Information Comissioners Office, 2015)

This case happened in 2015, however in 2018 the Data Protection Act was 'replaced' by the EUs General Data Protection Regulation (GDPR) which governs data protection requirements across the European Union (Swinhoe, 2019), GDPR outlines 7 principles (Information Commissioners Office), which are very similar to the DPA 1998.

- **Lawfulness, fairness, and transparency**
- **Purpose limitation**
- **Data minimisation**
- **Accuracy**
- **Storage limitation**
- **Integrity and confidentiality (security)**
- **Accountability**

In the UK, these principles are enforced using an updated Data Protection Act (Government, Your rights and the law - Data Protection, 2021).

Another mention is the Human Rights Act, article 8, which details a person's right to a private life, it is often cited in cases like these where a person's privacy may be impacted due to inappropriate data handling (Government, Human Rights Act, 1998).

2. Staysure.co.uk Architecture

The below diagram is an example of what the staysure.co.uk network might have looked like at the time of the breach. In the ICO report it mentions that the hackers were able to access the data via a vulnerability in Staysure.co.uk's application, the entry point is highlighted using the biohazard symbol.

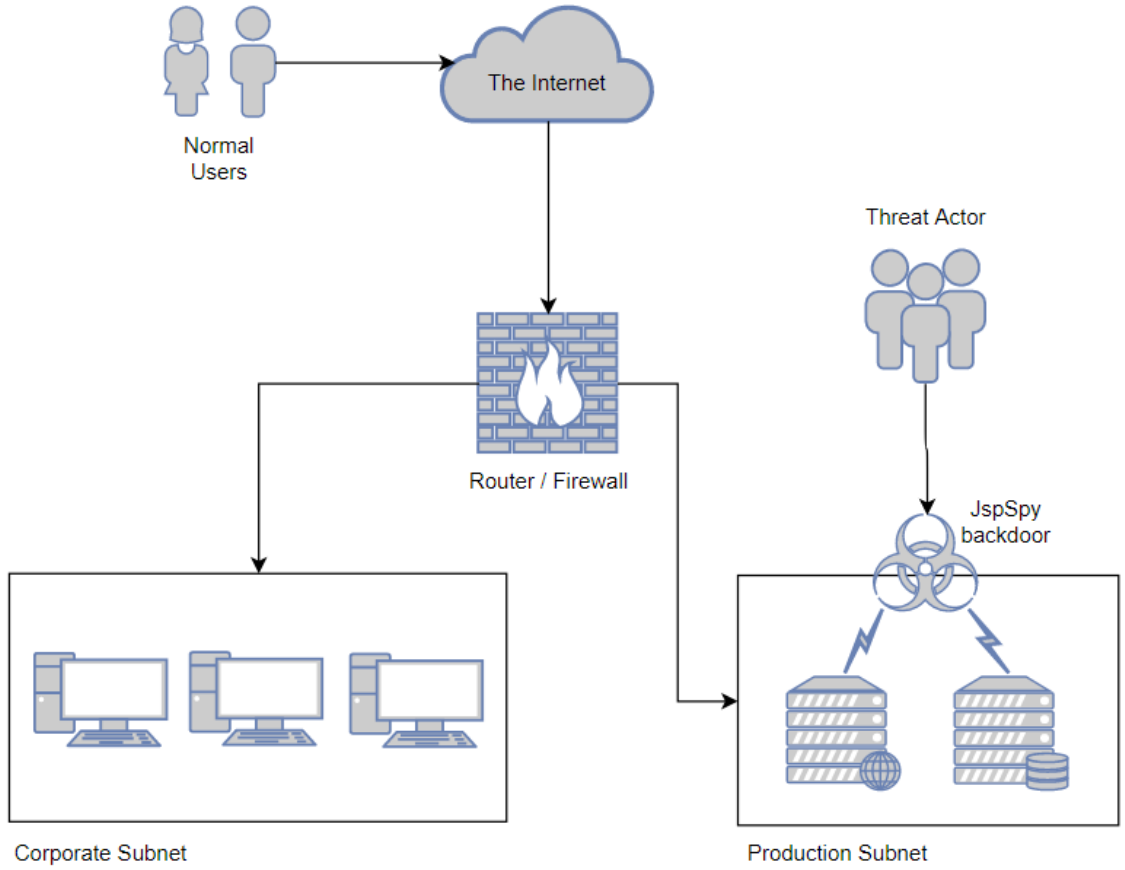


Figure 1 Assumed network architecture of Staysure.co.uk at the time of breach

The vulnerability existed in a piece of software called JBoss, JBoss is an open-source application server platform, and it is used for deploying and hosting Java applications (Red Hat). According to the ICO report a CVE entry was created for the vulnerability back in 2010, and a patch was released to fix it (Information Comissioners Office, 2015). In the 3 years from release of the patch Staysure.co.uk failed to apply the available update, leading to the conclusion that they did not have a formal plan for patch management and application.

There were 2 remote code execution vulnerabilities for JBoss submitted in 2010, CVE-2010-3708 and CVE-2010-1871 (MITRE, 2010)

The vulnerability allowed the hackers to install a piece of software called JspSpy which is a trojan that enables hackers to run commands on a remote system (TrendMicro, 2018), they were then able to use this to access other servers within the Staysure.co.uk production network.

3. Risk Assessment

I would recommend that Staysure.co.uk have a penetration test of their network performed by an accredited company who can properly evaluate the risk based on what they find and provide tailored remediations, however I have tried to summarise some of the most pertinent risks when dealing with internet facing applications.

Highlighted below are the most important issues discussed on their potential to breach the CIA triad:

3.1	Financial data is being stored incorrectly	Encryption is one of the key methods of preserving both a data's integrity and confidentiality, by storing sensitive data in cleartext anyone can see it, and thus anyone can modify it, this includes external attackers or an insider threat. This means there is a real threat of reputational damage and not to mention it is a breach of the PCI DSS standards.
3.2	Poor cyber education	It is my opinion that Staysure.co.uk has a very low cyber security maturity, the employees likely do not undertake regular cyber security training and that leaves them at risk of social engineering, more specifically phishing attacks. This is a real problem that might not seem important now, but if a piece of malware were delivered via a phish could comprise the confidentiality, availability and integrity of all of Staysure.co.uk's data.
3.3	Access to database via injection	A vulnerability of this type within the application allows for the confidentiality, integrity, and availability of the data to be compromised by an attacker. The implications of this can be severe, both from a reputational and legal perspective. The General Data Protection Law / Data Protection Act 2018 could also be in breach if such information can be compromised (Williams, 2021).

Read more on the CIA triad in Appendix 1.

ID	THREAT	VULNERABILITY	ASSET	IMPACT	LIKELIHOOD	RISK	NOTES
3.1.	Financial data is being stored incorrectly	No encryption on information in the database	Customer credit card information	5 - Card details can be used to make fraudulent transactions	5	CRITICAL	
3.2.	A backdoor is delivered via email	No user awareness of security making social engineering easy.	Staysure.co.uk's network, customer details & data	5 – Malware could allow an attacker to access systems and potentially encrypt data until a ransom is paid.	5	CRITICAL	94% of malware is delivered by email (TowerGate Insurance, 2020)
3.3.	Access to database via injection	Unsafe queries in source code can be vulnerable to SQL Injection attacks	Customer & Financial Data	5 – An SQL Injection attack could allow an attacker to all of the data in the database & even allow code execution.	5	CRITICAL	SQL Injection attacks represent 65.1% of all web application attacks (Akamai, 2020).
3.4.	Personally identifying data can be accessed or modified	No segregation or security controls on database server	Customer personal details	5 – Breach of data protection act, severe impact to customer confidence	5	HIGH	
3.5.	Storing CVV Numbers	CVV are stored in the database	All encrypted data	5 – Breach of PCI DSS standards, allows credit card data to be used fraudulently	5	HIGH	

ID	THREAT	VULNERABILITY	ASSET	IMPACT	LIKELIHOOD	RISK	NOTES
3.6.	Using an application with known vulnerabilities	JBoss contains a vulnerability which allows remote code execution on the server.	JBoss Application Server	5 – Allows direct entry into the main network where financial data is stored.	4	HIGH	65% of SMEs suffered a cyber attack from 2019-20 (Ascentor, 2020).
3.7.	No defensive mechanisms in place to detect intrusion.	No defensive mechanisms make a network easy to compromise.	Staysure.co.uk's network	4 – Makes disaster recovery difficult and gives the attacker more time on the network.	5	HIGH	26% of SMES have no cyber security measures in place at all. (TowerGate Insurance, 2020)
3.8.	Weak Encryption	Weak encryption algorithms used or encryption keys accessible to unauthorized users.	Encrypted data	4 – Easy to access keys would enable an attacker to decrypt any data found.	4	HIGH	
3.9.	Non-existent network segregation	No segregation of networks, servers containing sensitive information accessible to all on the network.	Staysure.co.uk's network	4 – No network segregation allows attackers to laterally move between servers with ease.	4	HIGH	
3.10.	Weak Passwords	No user awareness of security so weak passwords is used to access customer information.	Customer data	3 – Attackers can used password crackers to find and use weak passwords.	4	MEDIUM	51% of people use the same passwords for both their work & personal accounts (DataProt, 2021).

ID	THREAT	VULNERABILITY	ASSET	IMPACT	LIKELIHOOD	RISK	NOTES
3.11.	Employees can bring their own devices to work	An employee's mobile phone or laptop is infected with malware.	Computer Systems	3 – Malware bought in by a personal device could spread to production servers rendering them hacked, or useless.	3	MEDIUM	87% of businesses are dependent on their employee's to access business apps on a personal device (TechJury, 2021)
3.12.	Denial of Service Attack	Staysure.co.uk's network has a single entry point which is for ingress and egress traffic	Staysure.co.uk's network	3 – A DDoS attack could bring down Staysure.co.uk's whole network meaning employees could not access the web, and the website might go down.	3	MEDIUM	On average, the cost of a DDoS attack for SMEs is £120,000 (Kaspersky, 2017).

4. Recommendations

To prevent a future breach of this nature I would recommend that Staysure.co.uk implement the following security controls:

- **Create & implement an application patching policy**

It is unacceptable that the vulnerability exploited received a publicly available patch 3 years before the breach, although patching the software may not have thwarted the attack in its entirety, it would have made it much more difficult to do and Staysure.co.uk may not have been such a low hanging fruit.

I would recommend Staysure.co.uk take an inventory of their network, including servers, mobile devices & laptops, this inventory should include information on the operating system running, and what version of software is installed. Next, this inventory should be categorized into priorities, internet facing servers should be of a Critical priority, whereas office machines or printers might be Lower, the higher the priority the quicker any available patches should be applied.

Prioritization and timing are two important factors in patch management, therefore once prioritization has happened a regular time should be scheduled for that patching maintenance, this should be coupled as closely as possible with official software releases, for example, many big companies such as Oracle, Microsoft, and Adobe release on 'Patch Tuesday', which is the 2nd Tuesday of the month (Trend Micro, 2006), for this reason Staysure.co.uk might chose to apply patches on the following Tuesday, to allow time for testing.

- **Properly Segregate the network**

If Staysure.co.uk had a network that was properly segregated a compromise on their public web server may not have been so bad. The real issue with the Staysure.co.uk hack was that the breach on their public web server had direct access to databases containing very sensitive customer data.

Most large networks have a Demilitarized Zone. The DMZ is where all the public facing applications sit, firewalled off from the private network, the idea being that if an attacker were to make it onto the network via one of these applications they would be isolated in the DMZ and not have access to any data in the private network.

Better than implementing a DMZ would be to use a cloud service such as Amazon AWS or Microsoft Azure, many cloud providers have canned services for running secure databases & web sites and facilitating secure traffic between them, an example being Googles Cloud SQL and Googles Cloud Storage.

- **User Education & Security Awareness**

Due to the non-existent patching policy and poor attitude to data handling I am confident the cyber maturity of Staysure.co.uk is low, and I question their receptiveness to phishing attacks, therefore I recommend that Staysure.co.uk provide their colleagues with good data security and data management training.

- **PCI DSS**

I recommend that Staysure.co.uk get up to date with the PCI DSS standard because the practice of storing CVV numbers in the database is strictly forbidden and should never have been done.

The CVV number of a credit card is the important piece of information that is supposed to prove the person using the card is the card holder themselves, by storing this data they not only rendered its purpose useless but gave it to a malicious actor.

- **Encryption**

I recommend that Staysure.co.uk implement encryption on all their databases with immediate effect. Encryption's purpose is to securely protect data from unauthorized access, without encryption anyone with access can view and modify the data breaching the confidentiality and integrity of it, potentially making what is a already a breach, a much more severe one.

Depending on Staysure.co.uk's exact requirements there are a number of popular databases that make encryption easy to configure & use, two examples being PostgreSQL (PostgreSQL, 2020) and MySQL (Oracle, 2020).

Better than using a self-hosted database server would be to use a cloud provider service, AWS Relational Database Service (RDS) facilitates the use of encryption using keys that are managed using its Key Management System (KMS) which means the system administrators workload remains low, using AWS RDS also means all backups and snapshots are also encrypted, so you do not need to worry too much about data leakage via those avenues.

- **Incident Response Capability**

Although a full incident response capability is overkill for Staysure.co.uk at their current size, I would recommend they implement some sort of intrusion detection system, or IDS. An IDS is a software application that monitors a network for any policy violations, for example, Staysure.co.uk could ask an IDS to flag on read activity on the database any time after 9pm, at 9pm most employees are at home in bed, so activity after that time might suggest it was of malicious intent.

It is not enough for Staysure.co.uk to just implement the IDS, but they must also have a procedure for investigating and thwarting any attacks.

- **Web Application Firewall**

A WAF sits between the users of a web application and the application itself; its job is to filter and monitoring all traffic going through it. WAFs are normally very good at preventing web attacks such as Cross Site Request Forgery, Cross Site Scripting and SQL Injection however is not supposed to protect against all attacks and although it may not have prevented the attack in Staysure.co.uk's case its still a very useful tool and a control that I recommend that Staysure.co.uk implement.

5. Psychological Motivations

There are several reasons that hackers 'hack' and it largely depends on what type of threat actor they are, there are Nation States, who's motivations are purely political and might include sewing discourse or manipulating an election, there are also cyber criminals, who do it purely for profit, and there are Insider Threats, who's discontentment with their employer has led them to that point (Security, 2020).

Staysure.co.uk is a financial and insurance firm, which means it is very likely to be a target for Cybercriminals, who are generally looking for data that they can sell or ways of making fraudulent transfers, Staysure.co.uk holding lots of credit card data would fit the bill quite nicely for this especially so being a small business and therefore considered a low hanging fruit (PortSwigger, 2019).

FIN6

Aliases: Magecart Group 6, SKELETON SPIDER, ITG08

Targets: Financial Institutions, Hospitality & Retail

Techniques Used: T1134, T1087, T1560, T1119.. etc

FIN6 is a cybercrime group that has stolen payment card data and sold it for profit on underground marketplaces. This group has aggressively targeted and compromised point of sale systems in the hospitality and retail sectors (MITRE, 2020).

Another top threat for Staysure.co.uk will be Hacktivists. Hacktivists look for ways that they can embarrass the victim company and gain publicity for their cause, although I am not aware of any reason Staysure.co.uk might be personally targeted, their association with the financial sectors puts them at risk, perhaps in a case where another financial institution attracts infamy.

Anonymous

Aliases: ?

Targets: Scientology, Westboro Baptist Church, NSA

Techniques Used: ?

Anonymous is a decentralized & international hacktivist group widely known for various large scale cyber-attacks taking place under their name, this group has targeted various churches it believes to be cults or hateful in nature (Dibbel, 2011), as well as targeting the NSA for its threats to free speech on the internet (Waqas, 2013).

It is possible that Staysure.co.uk could also be targeted by APT groups, APT stands for Advanced Persistent Threats and it is the name given to threat groups that work with the sponsorship of a government. APT groups are normally very stealthy, and every major business sector has recorded cyber attacks carried out by advanced actors, whether their goal is to steal, spy or merely disrupt operations (FireEye, 2019).

admin@338

Aliases: ?

Targets: Financial Services, Trade & Economic Policy

Techniques Used: T1087, T1059, T1203,, T1083 .. etc

admin@338 is a China-based cyber threat group. It has previously used newsworthy events as lures to deliver malware and has primarily targeted organizations involved in financial, economic, and trade policy, typically using publicly available RATs such as PoisonIvy, as well as some non-public backdoors (MITRE, 2020).

In the case of what happened to Staysure back in 2013 I am confident that it was probably more of a Cybercrime type threat actor, due to the nature of what Staysure.co.uk do and their access to lots of credit card data, they would have been a very valuable target for a criminal group and its likely that data would have sold for a good price on the dark web, as well as the data itself being usable for fraudulent transactions.

However, something that every business is at threat of is an Insider Threat, an Insider Threat is one which comes from people within the organisation, and could be those who have insider information concerning the businesses security practices or detailed knowledge of the businesses network, most insider threats can be sorted into 3 categories (FBI, 2014):

- **Malicious Insiders:** Someone who knowingly used business confidential information to inflict harm to an organisation, this could be revenge for a pass on a promotion, a disagreement about pay or perhaps a redundancy or a firing.

- **Negligent Insiders:** This is likely to be someone who disregarded a very important policy (perhaps a data handling or encryption policy) which puts the organisation at risk, often without considering the impact of what they were doing.

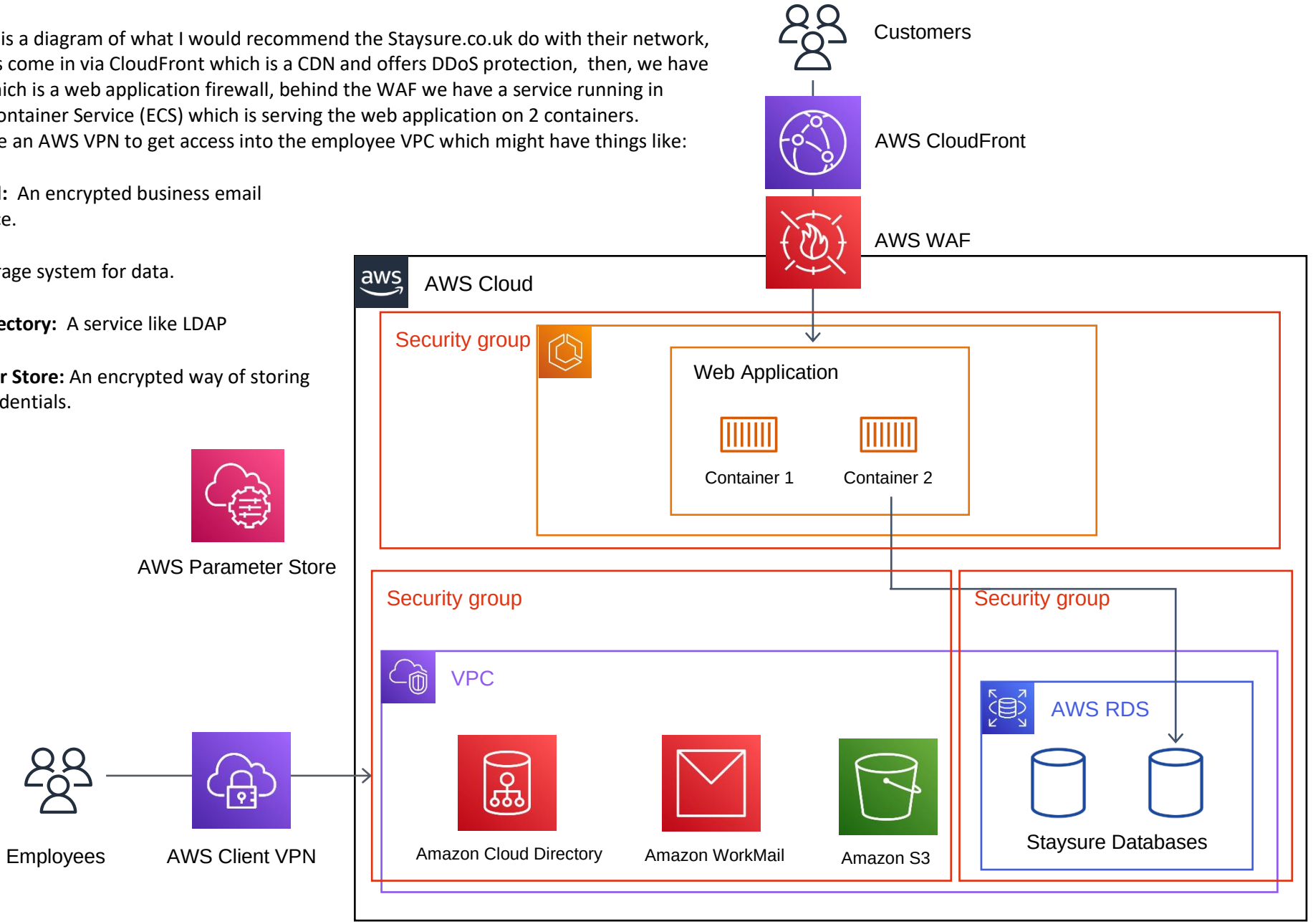
- **Infiltrators:** This might be someone who has infiltrated the company, perhaps by using credentials socially engineered, or in an extreme case someone who joined the company with the intent to become a malicious insider.

Due to the low security maturity of Staysure.co.uk as a whole, if this were a case where an Insider Threat was a factor, it would likely be a negligent insider, it could be that someone disobeyed the patching policy, which left the server open to the vulnerability, or it might be something as ridiculous as having a conversation about Staysure.co.uk's infrastructure within a public chat forum.

6. Security Assurance

The following is a diagram of what I would recommend the Staysure.co.uk do with their network, the customers come in via CloudFront which is a CDN and offers DDoS protection, then, we have AWS WAF, which is a web application firewall, behind the WAF we have a service running in AWS Elastic Container Service (ECS) which is serving the web application on 2 containers. Employees use an AWS VPN to get access into the employee VPC which might have things like:

- **WorkMail:** An encrypted business email and service.
- **S3:** A storage system for data.
- **Cloud Directory:** A service like LDAP
- **Parameter Store:** An encrypted way of storing secret credentials.



Cloud Infrastructure

- **Cost Efficiency:** I choose to use cloud infrastructure because cloud compute is cost effective, Staysure.co.uk will not have to lay down any money upfront for hefty servers or new and expensive firewalls because AWS will take care of that for them, they merely design the network they want and receive monthly bills for any data, compute, or extra services they have used. This frees up budget to be used for security or data protection training, as well as taking away any time spent configuring bare metal servers, leaving the network admin time to concentrate on those all-important security policies.

- **Disaster Recovery:** Cloud Computing also makes disaster recovery less expensive and much easier; AWS Backup enables you to completely automate the backup process and gives you the option to recover all your data at the click of a button.

- **Efficiency:** The ability to deploy many different services via one portal makes creating & configuring a security network much quicker to do, Staysure.co.uk will not have to wait for servers and firewalls to be configured, and it also means extending the network is much easier, if another database is needed, it takes merely 5 minutes to configure and deploy.

- **Security:** In an on-premises network, you would need to purchase & configure multiple firewalls for each network segmentation you wanted to create, however via VPCs and Security Groups AWS allows you to shut off parts of the network virtually and all you must do is define your inbound and outbound rules via the UI, making it efficient & easy to do!

- **Logging:** AWS allows you to configure all your services to log to CloudWatch, CloudWatch is a portal for storing, viewing and search through logs, having a centralized logging platform for all services helps in the case of a breach, as it allows Staysure.co.uk to see exactly what was accessed, and by what user.

- **Access Management:** Cloud Computing services have very granular permissions when it comes to what a user can do, for example you can give an employee access to WorkMail but not S3, you can also stop them seeing single files within S3, you can even give them access to workspaces, which means they cannot access anything unless they are on a locked down machine in the VPC, , if configured well it means if Staysure.co.uk did ever get breached the attacker probably would not be able to access anything anyway.

- **Encryption:** Most AWS services provide encryption of data by default and with no extra configuration, meaning if Staysure.co.uk were breached again, the hacker would not be able to read any of the data (AWS Security, 2020).

Containerisation

Containerisation has been a hot topic for a long time, and the reason I used Amazon ECS to host the web application was to capitalize on some of the benefits of containers:

- **Scalable:** Containers have low overheads, because they are not running a whole operating system they are quick to start up and because they run single services (Humantic, 2020), if

one goes down you just boot up another one, the alternative being taking a few hours to rebuild and configure a server.

- **Portable:** Containers allows you to define & run the base dependencies for an application, so if you had postgres 7, and your colleague had postgres 5, you could both run a postgres 6 container, because the container would handle downloading & running that service for you, this prevents situations where an application may behave differently on different versions of a dependency.

- **Flexibility**: Running your services in containers gives you the benefit of being able to switch between clouds such as AWS, GCP & Azure easily because they all have their own containerisation platforms, whereas the alternative would be hours spent recreating all your servers.

- **Isolation:** In Amazon ECS containers run in isolation, they have their own VPC and by default they cannot talk to any other containers (Docker, 2020), meaning if your container did get compromised the attacker would have very limited places to go, especially if you had great security groups and made good use of the AWS parameter store.

7. Information Security Policies

7.1. Encryption Policy

7.1.1. Purpose

This policy exists to provide guidance on where and how encryption should be applied effectively across the organisation.

7.1.2. Scope

The policy applies to all Staysure.co.uk employees and affiliates.

7.1.3. Policy

1	All Staysure.co.uk being transmitted between internal systems should use the Staysure.co.uk VPN at all times without needing to be encrypted.
2	If any information classified CLIENT CONFIDENTIAL and above is being sent outside of internal systems, including methods such as email, storage on an external drive, and uploads to websites, it should always be encrypted.
3	High Risk or Sensitive data should never be processed in public areas such as coffee shops or on train journeys.
4	All Staysure.co.uk owned devices should be encrypted using the operating systems full volume encryption system, for example BitLocker, recovery keys will only be available for IT Administrators.

5	When encrypting anything you should use Staysure.co.uk's facilities for doing so, never external sites or services.
6	Any encryption algorithms used must meet the standards defined in NIST FIPS 140-3 (NIST, 2019)
7	Any cryptographic keys must be generated and stored in a secure manner that prevents loss or compromise.
8	Cryptographic key generation must be seeded from an industry standard random number generator, you can see a list of those approved in NIST FIPS 140-2 Annex C (NIST, 2001).
9	All databases and data which is at rest should be encrypted.

7.1.4. Compliance

Compliance will be verified regularly, and all outgoing files will be subject to checks, regularly audits will take place to ensure this policy is adhered too.

Any exceptions to the policy will need several rounds of approval by the security team and non-compliance may render that employee subject to disciplinary action.

7.1.5. Related Standards

- NIST FIPS 140-3
- NIST FIPS 140-2

7.2. Patch Management Policy

7.2.1. Purpose

This policy defines the procedures that should be followed for patch management within Staysure.co.uk.

7.2.2. Scope

The policy applies to all Staysure.co.uk employees and affiliates and all Staysure.co.uk technology assets, this includes, but is not limited too:

- Windows & Linux Servers
- Databases
- Web Application Servers
- Firewalls & Access Points

7.2.3. Policy

The following table defines the timeframes at which patching is supposed to take place depending on the vulnerabilities risk rating.

VULNERABILITY RISK RATING	CLOUD SYSTEMS	EXTERNALLY EXPOSED	INTERNAL SYSTEMS
CRITICAL	5 days	5 days	15 days
HIGH	5 days	5 days	15 days
MEDIUM	15 days	15 days	30 days
LOW	Whenever convenient.	Whenever convenient.	Whenever convenient.

7.2.4. Compliance

Non- compliance to this policy can potentially be very damaging for Staysure.co.uk, so in the case any contractor or employee is found in breach of this policy they are at risk of disciplinary action.

7.2.5. Related Standards

- ISO/IEC 27001:2013 standard, control A.11.2.7

7.1. Breach Response Policy

7.3.1. Purpose

This policy defines the procedures in place for responding to and recovering from a breach.

7.3.2. Scope

The policy applies to all those within Staysure.co.uk that collect, access, maintain and protect any personally identifiable information.

7.3.3. Policy

1	As soon as a breach is identified the dedicated incident response working group should be informed, the dedicated point of contact for this group is Jessica Williams.
2	All information that points to a data breach should be collected and made available to the working group.
3	All information relevant to the breach should be collected, grouped together and stored in a dedicated folder on the Staysure.co.uk shared drive, this should be provided to forensic investigators if necessary.
4	A communication plan should be put together to adequately explain the breach to both internal employees and any press contacts who are asking for a response.
5	All employees must engage with and provide any help necessary to investigate the breach.

7.3.4. Compliance

If any employee is found in breach of this policy, they are at risk of disciplinary action, which includes termination of employment.

7.3.5. Related Standards

- ISO/IEC 27001:2013 standard, control A.12.1

8. Appendix A: The CIA Triad

CIA stands for Confidentiality, Integrity & Availability, it is a very simple but widely flexible security model that works on 3 principles:

Confidentiality

Confidentiality refers to efforts to keep data private or secret. In practice, it is about controlling access to data to prevent unauthorised disclosure. Typically, this involves ensuring that only those who are authorised have access to specific assets and that those who are unauthorised are actively prevented from obtaining access.

Integrity

Integrity is about ensuring that data has not been tampered with and, therefore, can be trusted. It is correct, authentic, and reliable. Ensuring integrity involves protecting data in use, in transit (such as when sending an email or uploading or downloading a file), and when it is stored, whether on a laptop, a portable storage device, in the data centre, or the cloud.

Availability

Systems, applications, and data are of little value to an organisation and its customers if they are not accessible when authorised users need them. Put simply; availability means that networks, systems, and applications are up and running. It ensures that authorised users have timely, reliable access to resources when they are needed.

9. Works Cited

Akamai. (2020). *State of the Internet.*

Ascentor. (2020). *Cyber security myths putting SMEs at risk.*

AWS Security. (2020, June). *The importance of encryption and how AWS can help.* Retrieved from AWS Security Blog.

Commission, E. (n.d.). *Rules for businesses and organisations.* Retrieved from Official website of the European Union: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en

COX Blue. (2020). *DDoS Statistics.*

DataProt. (2021). *Save Your Data with These Empowering Password Statistics.*

Dibbel, J. (2011, July). Sympathy for the Griefer: MOOrape, Lulz Cubes, and Other Lessons From the First 2 Decades of Online Sociopathy. *GLS Conference*.

Docker. (2020). *ECS Integration.* Retrieved from docs.docker: https://docs.docker.com/cloud/ecs-integration/

Dutton, J. (2015, February). Staysure fails to comply with the PCI DSS and is fined £175,000 by the ICO. *itgovernance*.

FBI. (2014). *FBI Counterintelligence: The Insider Threat. An introduction to detecting and deterring an insider spy.*

FireEye. (2019). *M-Trends Cyber Security Trends.*

FireEye. (2020). *Cyber threats to the financial services and insurance industries.*

Government, U. (1998). *Data Protection Act 1998.* Retrieved from legislation.gov.uk: https://www.legislation.gov.uk/ukpga/1998/29/contents

Government, U. (1998). *Human Rights Act.* Retrieved from legislation.gov.uk: https://www.legislation.gov.uk/ukpga/1998/42/schedule/1/part/I/chapter/7

Government, U. (2021). *Your rights and the law - Data Protection.* Retrieved from www.gov.uk.

Humantic. (2020). *Benefits of Containerization.* Retrieved from Humantic: https://humanitec.com/blog/benefits-of-containerization

Information Comissioners Office. (2015). *Monetry Penalty Notice - Staysure.co.uk.*

Information Commissioners Office. (n.d.). *Guide to the General Data Protection Regulation (GDPR).*

Kaspersky. (2017). *IT Security Risks Survey* .

MITRE. (2010). *Common Vulnerbility & Exposures Database*. Retrieved from Common Vulnerbility & Exposures.

MITRE. (2020). *admin@338*. Retrieved from MITRE ATT&CK: https://attack.mitre.org/groups/G0018/

MITRE. (2020). *FIN6 - G0037*. Retrieved from MITRE ATT&CK: https://attack.mitre.org/groups/G0037/

Newsdesk. (2015, February). Broker fined £175,000 by information watchdog after cyber criminals raid customer records. *Insurance Times*.

NIST. (2001). Approved Random Number Generators Annex C. In N. I. Technology, *FIPS 140-2.*

NIST. (2019). *Security Requirements for Cryptographic Modules.*

Oracle. (2020). *MySQL Enterprise Encryption.*

PCI Security Standards Council. (2018). *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures .*

PortSwigger. (2019). Low-hanging fruit: Cybercriminals increasingly targeting small businesses. *The Daily Swig*.

PostgreSQL. (2020). *PostgreSQL 13 Encryption Options.*

Red Hat. (n.d.). JBoss Enterprise Application Platform data sheet.

Security, C. C. (2020). *Cyber Threat and Cyber Threat Actors.*

Swinhoe, D. (2019, August). GDPR vs UK Data Protection Act 2018: What's the difference? *CSO Online*.

TechJury. (2021). *41 Stunning BYOD Stats and Facts to Know in 2020.*

TowerGate Insurance. (2020). *SMEs & Cyber Attacks.*

Trend Micro. (2006). *Patch Tuesday... Exploit Wednesday.*

TrendMicro. (2018). *TROJAN.JAVA.JSPSPY.A.* TrendMicro.

Waqas. (2013, November). Anonymous Declares Global Cyber War on U.S. Government against Hammond's Sentence and NSA Spying. *HackRead*.

Williams, J. (2021). *Penetration Test of Global Software Web Application.*