BESPOKE INTERNATIONAL TRAVEL (FRANCHISES) LTD

Computer Security

CP60028E

Module Leader : Colin Beeke

Pouya Shahverdi Moghaddam

ID:21245645

Abstract

As technology advances at a fast rate, organisations are tasked with dealing with the increased chances of security attacks that can be malicious or non-malicious. For this module I am tasked with researching the many threats and vulnerabilities that exist in 2019 with recommendations and ways for the enterprise that can deal with such issues. Furthermore, this will report will also produce policies, sub policies and recommendation that will help the enterprise whilst starting up.

Table of Contents

Introduction

In this assignment I am tasked with working as a "Computer security consultant", working for a firm of independent computer security system advisers. The specific task in hand in to compile a report that will investigate the current computer security threats that would exist to a new Enterprise start up that would like to operate from the United Kingdom

The report will then be used by the company as a top-level security policy that will be then be used and developed upon by the enterprise as the basis of their main reference source for the computer security manager and the staff.

This report's main task will be to identify the major threats and vulnerabilities that are present for such a firm as well as being able to categories the risks with solutions or an internal process that would help the business.

The report must also include details that would enhance the security operations that should already be in place and ensure that there is also compliance with the various regulatory requirements that are in place as well as newer ones such as GDPR.

The report will consist of ten different threats that could affect the security of the company and will then go into detail regarding the vulnerability and the countermeasures available to deal with such issues. It will then go into detail about the prioritization of each threat with a frame work in place that will discuss the key top policies and the sub policies with the report further moving on to the compliance and legal regulatory issues the company will need to follow in order to be able to work in the EU and internationally. The report will finish with a conclusion of the findings and some final recommendations.

Case study

Bespoke International Travel (Franchises) Ltd (BIT)is a new Enterprise start up proposal. They will operate from the United Kingdom and looking to franchise within the United Kingdom. They all aspire to work within Europe and globally.

Bespoke International Travel (Franchises) Ltd. The Enterprise will be based within the United Kingdom but looking to open Franchises throughout the United Kingdom, Europe and then globally. The monitoring will be automated as much as possible through electric systems and supported through a call centre staffing approach. The concept is that a client can arrange a bespoke holiday with a local franchised partner. For example, if a Portuguese couple wished to go to China and visit a number of their selected sites with a personal trip guide then they would go to the company website select the local franchised partner and they would then organise the trip through a personised approach. The local franchisee partner could be a local resident that has retired but offering such services and needs the support and facilities of a large enterprise.
The company does not see itself as organising trips but more of facilitator to the various franchised businesses that operate under its licensed arrangements.

Threats

A threat is a potential occurrence, malicious or otherwise that may harm an asset. Threats can occur for a number of reasons within a corporation and it is important that such things can be identified in advance in order to prevent large scale damage.

There are many types of threats such especially cybersecurity threats and depending on the enterprise and its target audience we can categories the threats in different ways, with cyber-attacks being at the heart of most of the malicious attacks. Cybersecurity reports by Cisco shows that 31% of organizations have at some point encountered cyber-attacks on their operations technology.

In order to be able to identify the relevant and correct types of threats we have to look more into the company we are dealing with the type off staff and also their customer base.

Bespoke International Travel (Franchises) Ltd will be dealing primarily managing two different types of staff/partners, these will be call centers and the localized franchise partners. This will mean that we are dealing with internal and external members of staff and for that we have to take into account the types of security access the staff will have and the affect it could have with regards to cyberattacks as well as taking into account times where the franchise partners will be accessing the system or using unsecure or unsafe systems that can cause potential issues. We have to also consider that some of the local franchises are retirees, this can mean a number of things such as if their general computer knowledge is up to date or if they are using secure devices to work from etc. We have to take all of the above into consideration when we choose the threats for Bespoke International Travel (Franchises) Ltd.

Based on current 2019 research and the Enterprise needs these are the following threats that needs to be studied for Bespoke International Travel (Franchises) Ltd

- Data Breach
- Distributed denial of service (DDoS) attack
- Malware Attack
- Loss of Data
- Insider Threats
- Unsecured IoT Devices
- Phishing Schemes
- Cloud cyber security threats
- Cryptojacking
- SQL injection

Data Breach

The average data breach in 2019 will cost an enterprise on average $1.23 million and a SMB (small medium business) being 120k and the cost rapidly increasing according to the Kaspersky Lab, this is a 24% increase from 2017 for enterprises and 36% increase for SMB. These attacks have become so widespread that a growing number of consumers and employees have accepted data breaches as an inevitability. (Canner, 2018).

A breach can primarily happen for a number of reasons, outside malicious attacks caused by hackers. Lack of security culture within the enterprise and employees working within the company can be one of the main factors for data breach.

How can it affect us?

As discussed, we have seen the affects a data breach can have on a vulnerabilities enterprise like Bespoke. There are many vulnerabilities but with technology advancing in today's world. For that reason, a strong security team is required to act to prevent data breaches as well as creating a security system for IT system BIT will be using. A lack of security culture can cause a huge loss in money and revenue due to the following:

- Loss of business
- Penalties and fines
- Hiring new staff
- Improving software and infrastructure
- Employing external help

Vulnerabilities

Vulnerabilities within an enterprise can make data breach easy. One of the most common is staff, both malicious and non-malicious At times data breaches can occur due to the lack of attention by staff. Lack of password for data as well as lack of encryption for data is a major cause for concern. Staff need to have their privileges checked to see if they have the rights to access certain data.

Countermeasures

A Number of security policies need to be in place to train staff with constant updates in order to defend against new attacks.

System patches and updates should be checked prior to installation to check for any signs up weakness that would allow attackers an access point.

Using a reputable cloud data storage provider should is also important as attacks on virtual machines can occur on the cloud storage.

Employers should be trained to follow the security policies and be kept vigilant to prevent and spot out any protentional losses.
Employers should be made aware of the data protection act 2018 as well as GDPR and made aware of the coconscious of data breach.

SQL Injection Attacks

SQL Injection attacks is one of the many ways malicious attacks take place on enterprises that run a database. These attacks take advantage of dynamic SQL. Dynamic SQL is a SQL statement that accepts input from users directly (Gibson, 2015). These days many websites need the user to enter text in a text box or in the web address, the user will be able to supply data that is used directly in a SQL statement and this is where the SQL injection attack can occur. Instead of giving the expected data that is required, SQL injections attacks use a different string code. This code has the chance to bypass and compromise the database. There are a number of ways to combat this type of attacks quite easily and with the use of parameters and stored procedures that review the code.

How can this affect us?

As Bespoke International Travel (Franchises) Ltd will be a website for customers to book their holidays using an automated electronic system, we have to assume that the system will have a website and database used for storing information of the customer contact details for the franchisees to contact as well as the possibility of payment details stored on the database. An SQL injection attack can have a massive effect on the enterprise as customer details can be stolen or the possibility of an entire database being deleted. This will in turn can cause customer loss, Fine and legal issues, bad PR, loss of money and business for Bespoke International Travel.

Vulnerabilities

The main vulnerability for this will be the programmer/database developers employed by Bespoke International Travel (Franchises) Ltd as attacks can easily be avoided by the use of parameters and stored procedures. Other vulnerabilities can be unauthorized access to the database in order to remove the data.

Countermeasures

There are a number of countermeasures we can put in place. The first and most important one would be the method used for employing the database developer. There should be a extensive interviewing process put in place with tests to see the ability of the developer. SQL injection attacks are easy to avoid by using parameters and stored procedures that first review the code, however all database developers aren’t aware of the risks (Gibson,2015).
Other countermeasures are audits used to review source codes, strong passwords for administrator accounts, making checks for privileges on accounts in order to avoid unauthorized access to the source code.

Distributed denial of service (DDoS) attacks

DDoS attacks are malicious attack known to disturb the traffic coming to a server, network or service by overwhelming the target by a flood of internet traffic. This is achieved by the utilization of multiple compromised computers or IoT devices. Criminals and attackers will be able to run botnets from a command and control system and are given a command to carry out an attack at any particular time. This increased influx of traffic will effectively cause the server to either slow down and make it harder for genuine users to access the site or it will cause a server crash. There are a number of different DDoS attacks, such as; Application layer attack, Protocol attacks and Volumetric attack.

How can this affect us?

Bespoke International Travel (Franchises) Ltd will be running website and servers for clients to make bookings. We have to also consider the companies aspirations to work in Europe and the future globally, with that comes the likelihood of attacks either from a number of sources such as criminals with certain motives or disgruntled employees, competitors or even customers who may have used the service in the past and were not happy. Depending on the goals and success of the attacker a loss of potential revenue as well as new cliental can ultimately have an effect on the enterprise.

Vulnerabilities

Vulnerabilities for DDoS attack depend if the organisation is using a public facing server, the servers have several potential weakness, however if you don't have any public facing servers, there aren't any vulnerabilities for the organisations (Gibson, 2015). As BIT will be using public facing servers to run its website, the main vulnerabilities are a lack of protection as well as intrusion detection systems in place that will be able to tell when a attack is happening.

Another vulnerability will be social engineering. In circumstances of an attack the awareness to spot the increased traffic and inform the ISP or the relevant people required to act.

Countermeasures

We can put a number of measures to avoid attacks. One of the measures is to use an intrusion detection system that will detect any questionable oncoming traffic. These systems are intelligent enough to spot out real traffic from the malicious type and they don't require any additional onsite hardware. There are different types of IDS such as a passive system that will log the threat and alert the users but the recommended IDS should be a active system that will modify and block the environment. (Gibson, 2015) Firewalls should be installed as well as routers configured to prevent attacks.
Another countermeasure should be training geared to all users in order to spot out attacks quickly and with the view to train all users on social engineering.

Phishing Schemes

Phishing attacks are one of the most common security challenges that both individuals and companies face in keeping their information secure. (Lord, 2019). These attacks can range in many different form, forms such as malicious emails, fake links, fake web forms, pharming with the ultimate aim of gaining access to systems, database, passwords, sensitive data etc. Attacks can be easily spotted as some of these attacks are not very sophisticated however on the other side of the scale some attacks can be very sophisticated to an extent of fooling experts in the field and for that reason this type of scam is very common and can be devastating to an enterprise.

How can it affect us?

As stated this type of attack is very common and according to Greg Scott, a security expert working for Infrasupport Corporation, “One key fact to remember when it comes to protecting against phishing attacks is...All it takes is one employee to take the bait.
In a company with, say, 1000 employees, that's 1000 possible attack vectors.” So the likely hood of an attack is very high and considering the enterprise is new and a start-up, criminals and hackers will be attempting to see how secure systems are as well as testing out the staff to see if they will fall for such attacks. Depending on the motives of the attacker and the sophistication of the attack a number of issues can occur to BIT but like major other attacks it can leave the Enterprise with major issues to deal with.

There are two way these attacks can affect BIT. One is for the attackers to steal sensitive data from the database of BIT which it turn can affect the enterprise in terms of fines, PR, loss of revenue and so on but another aspect would be the use of BIT and it’s information to create fake web pages, emails and links in order to trick unsuspecting customers or random individuals. Most of the time it will be the company’s original customer base falling victim of the fake emails thus creating a bad imagine for the enterprise as well as bad PR. So overall the damage to BIT can be quite big.

Vulnerabilities

Vulnerabilities for BIT can be a number of things. Lack of spam filter on emails, systems not running antivirus or the latest update and patch, the same applies to the system updates, employers lack of knowledge with phishing and how to sport out attacks, radiant emails, links and webpages. Encryptions for employers that are dealing with telecommunication as some phishing attacks can be made via the phone to the call centers. (lord, 2019)

Countermeasures

There are a number of countermeasures that can be put in place to avoid attacks. A up to date security policy in place that goes through the details of how to avoid attack as well as handling the aftermaths or ways to stop attacks going further. The security policy should also detail the latest phishing tactics used by criminals to stay one step ahead. Training employers as well as conducting mock phishing scenarios to familiarize employers. Keeping all systems and antivirus up to date with the latest patch to avoid attacks. Encryption of all data to protect sensitive data. Installing email filtering systems

Insider threats

Any business/enterprise let it be small or a multinational type company can experience from insider threats. This type threat can be responsible for as much as around 30% of all cybercrime according to various surveys (Sullivan, 2018).

These attacks can range in form and depending on the motives it can be a sabotage type attack, theft or fraud. For that reason, it is important to be vigilant during the employment stages and carry out a number of strategies in order to avoid or reduce the risk of these threats.

How can it affect us?

As shown that these types of attacks can be responsible for 30% of all attacks, this puts BIT at great risk, especially as a host of new employers that will start working with the company and the thought of having just one “bad apple” going through the system can cause devastating scenarios to the company. We also have to consider that some employers may simply become disgruntled at future dates after employment which makes the risk of this attack always high.

As BIT has wishes to enter Europe and the global market the possibilities of other competitors also employing a “Trojan horse” tactic shouldn’t be underestimated. These attacks can range in information technology sabotage as well as theft of intellectual properly and clientele information.

These types of attacks can make enterprises lose money as they are extremely expensive to deal with because some attacks can go undetected for long durations of time whilst slowly causing damage to the company. According to Ponemon Institute, the average cost of a insider threat to an organisation is at $8.76 million. These attacks also risk compliance with data protections acts as well as causing operational issues to a company. This could potentially put BIT out of business early on.

Vulnerabilities

Human error should be considered a big vulnerability when it comes to insider threats, especially with start up Enterprises as many of the initial employments are done either by the owners or a small team. We also have to consider the emotional sides of humans and their good natures as this could be classes as a weakness during the hiring process as it could make an employer skip or take the pre-employment background checks less seriously.

A lack of monitoring and logging of network activity done through a network administrator can cause issues because violations can be spotted through this method.
Lastly policies should be up to date, especially the insider threat protection policies. As the chances of having a policy that is not fair or even to every can lead to issues with employers.

Countermeasures

With all the points discussed in vulnerabilities we can put forward a number of important steps to remove or reduce the risk of attacks. The most important countermeasure to be put in as this is a start-up enterprise is the employment pre-checks. There should be checks done in the history of employers in all staff, as well is references, ID checks, criminal checks. There should also be tests on character and judgement of the person.

The monitoring system should be in place to alert if there is a security breach or activity that shows when a employer is doing something they shouldn't be doing.

As with all vulnerabilities, clear policies should be in place and reviewed with regular updates that will enable a clear security culture within the enterprise.

One last type of countermeasure we should also consider is to create a good working environment for employers, a large percentage of insider threats are caused by issues created due by either bad working environments.

A Bring Your Own Device policy (BYOD) needs to be set in place to monitor, authorized and make sure the devices the employers used cannot be used for attacks. This policy would make sure the security team at BIT have gone through enough measure and checks to allow staff to use their devices to prevent attacks such as infecting IT systems, installing spyware etc.

Malware Attack

“Enterprise Malware Detections Up 79%” according to DarkReading.com, this type of attack has seen an increase in the last few years and especially towards enterprises. The manner in which these attacks happen changed with the attackers taking a different approach. Their strategy involves more research into vulnerable businesses rather than random attacks in the hopes of attacks working. This and then made it easier for business that have a low-level security in place to get targeted and attacked.

Malware attacks work by “malware” or a specific type of malicious software that is installed on the victim’s computer or IT systems performing operations oblivious to the person or organization. This type of attack is mostly always malicious with the intendent of either stealing data/personal information or used in other criminal activity like mining.

The malware can infect the user’s computer in a number of ways such as infected IoT’s, spam email, bad links etc.

How can it affect us?

One manner in which Malware attacks has affect BIT is with the use of Ransomware. Malicious attacks towards businesses have employed the tactic of using ransomware, this is a type of attack where the attacker would request a ransom to “free” the infected computer with the attacker assuming the enterprise that has money is willing to happily listen to them. This type of attack was carried out on NHS England in recent years and caused a nationwide issue. “Delays caused by ransomware can be incredibly expensive, researchers say, especially when the victim has a wealth of infected endpoints and no backup plan in place. Incident response is costlier than paying up.” (Sheridan, 2019)

Vulnerabilities

Vulnerabilities for these types of attacks is mostly due to the system security of the enterprise and not allowing these attacks from occurring in the first place, the second line of defense is preventing the malware from actually infecting the computers and getting installed. Staff training is also another aspect and making sure the staff know the dangers of this attacks.

Countermeasures

As discussed above the countermeasures in place should be a strong security system. A firewall needs to be installed, updated regularly with patches to prevent new types of attacks and malware programs. An IDPS on the system to prevent attacks from happening with alerts of attacks and evasion of attacks. Lastly staff training in place with test to make sure they do not click on links, use IoA’s that can infect the system. All these should then be incorporated to security policies.

Unsecured IoT devices

IoT or Internet of things as it's known are devices that have an internet connection such as mobile phones, tablets, smart watches or any device with an internet connection etc. These devices are affectively a vulnerability for many organisations as attackers can use the devices and maliciously attack through them.

"A survey of some 700 product security professionals with responsibility for connected products. The survey, sponsored by the firm DigiCert, found wide disparities in the security of IoT devices, with the least secure devices six times as likely to suffer from online attacks."

Depending on the security of the device, application and operating systems, attackers will then hijack the device through a vulnerability such as outdated software, infected applications and plan their attack.

Over the years there have been many well-known attacks such as the Mirai attack which used a IoT botnet to attack websites like Twitter, Netflix etc.., the Jeep hack where the car was attacked through a security update that was done through a cellular network, The Owlet WiFi Baby Heart monitor attack where the webcam was hijacked and viewed by the attackers

How can it affect us?

This type of attack can affect BIT in a number of ways. Attackers can hijack camera's, webcams, phone cameras to snoop on the enterprise, other type of attacks can involve data loss and intellectual property. Infection of IT systems. Denial of service, ransomware etc

Vice President at DigiCert in charge of healthcare solutions. "Every single bottom tier company experienced a security misstep. They were six times as likely to experience a (denial of service) attack or data breach, more than six times as likely to have unauthorized access to an IoT device and 4.5 times as likely to be infected with malware or ransomware."

Vulnerabilities

The vulnerabilities with this type of attack can be categorized in two manners. We can have vulnerabilities for when an attack does occur using IoT's then we have to consider the typical security risk such as weak firewalls, lack of IDPS, unencrypted data but the main vulnerability to have in place to prevent an attack from occurring is a weak IoT security policy and training for the staff.

Countermeasures

Besides the typical security measure in place to protect the enterprise a security policy has to be in place that makes sure IoT devices are authorised, made sure to be updated regularly with the latest software and patches. Devices to be monitored with encryption of data going and entering the devices.

Cloud Cyber Security threats

With cloud technology being at the forefront for most enterprises a new type of attack that an enterprise has to get protected from is Cloud Cyber Security threats. These give attackers a wider range of attacks. It has become common practice for firm to move from physical servers for their data to cloud-based servers. This is due to a number of factors such as cost cutting, cutting down on number of staffs, space and cutting down the risks of using physical hardware, however in turn this has caused issues in terms of security. Many organisations that do move on to cloud based servers assume the risk of attack is lower due to the cloud providing firm's own security protocols and end up neglecting threats that can occur. This came in a survey where 450 firms where questioned and 73% them felt that public cloud was more secure than their own security (Zorz, 2019)

One of the biggest threats from cloud computing is IT shadow systems, this type of threat is non-malicious and to do with staff using un-authorised applications such as Evernote, iCloud etc. Other forms of attack can be malware attacks or virtual programs running alongside in the cloud to steal data.

How can it affect us?

This type of attack will affect BIT in terms of data loss or data breach. Staff could use shadow IT systems to remove data and personal information from the enterprise. Payment information of customers can be stolen. This can lead to fines for the enterprise, loss of money, trust in the enterprise being compromised. Loss of data from malware attacks is another factor

Vulnerabilities

The vulnerabilities for this can be the type of cloud service provider the enterprise decides to use and the level of security they employ. At times this can cause confusion between the security staff at the enterprise as and the cloud provider. Communication is another issue. When and if attacks do occur a good line of communication is needed between the enterprise and the provider.

In terms of security of the enterprise itself, password management can be an issue with protecting data.

Countermeasures

An research for a reputable cloud provider is important, this can make the job of the security team and CISO much easier. Making sure the system are updated and the latest patches are installed to prevent from attacks occurring. The possibility of employing a staff that just deals with the cloud servers can be beneficial. Staff audits to prevent the use of shadow IT systems being used in the enterprise is also important.

Cryptojacking

With the sharp rise in "Cryptocurrencies" such as Bitcoin and Ethereum, many people are looking ways to invest and getting a share of pie as they say. In order to fully understand how cryptojacking works we first must understand how crypto coins works. There are a number of ways to obtain these coins. They can either be purchased, be donated or be "mined". Coins can be buried or unavailable, miners can use a number of strong algorithms to obtain these coins, however these algorithms needs extremely powerful machines behind them and this is where cryptojacking comes into play. Criminals will use malicious code and software to infect the user's computer and use their machine without permission to mine crypto currently.

The sharp rise with this type of criminal activity according to Michael Nadeau from CSO online is "The simple reason why cryptojacking is becoming more popular with hackers is more money for less risk." Hackers also don't need a lot of skills for this type of activity as they can purchase cryptojacking kits from the dark web for very cheap.

How can it affect us?

Besides supporting criminal activity of hackers, Cryptojacking can compromise the IT and hardware systems of BIT in terms of power and performance as CPU's will be put under strain and used for mining. This in term slows down the systems of the enterprise and cause issues with staff, workability in the enterprise. The cost of electricity bills can run high as the machines are always performing at the peak and can run during the night.

Company reputation as well as regulatory dealings such as GDPR and data protection act, the ethical issues of using workers unknowingly to use for criminal activity.

Vulnerabilities

There are two main vulnerabilities in terms of falling for cryptojacking and both these deal with how to prevent your system getting infected. Criminals target users in two way, by either social engineering tactics to use phishing schemes which results in staff clicking on links and running a script or hackers inject scripts into popup adverts for the infected code to execute once it has been clicked on and thus mining on the users.

Countermeasures

Training should be provided to prevent social engineering for staff. Staff should also be taught the dangers and cryptojacking and how they can prevent it by avoiding malicious websites, links and adverts. The blocking of website that host JavaScript minors should be implemented as well as security measures in place to stop from minors running unauthorized programs on the system with the IPDS system configured. (Bradley, 2018)

Data Loss

Data loss can be a massive threat for any enterprise and can lead the business into big financial loss as well as reputation issues with 51% of companies closing down within two years of the loss.

Data loss can occur in a number of manners within an enterprise such as human error, viruses and malware, Hardware damage, power outages, theft, natural disasters, software corruption and hackers. Many of the threats listed in this report can lead to data loss so.

How can it affect us?

This can close down the BIT, many enterprises end up closing with as much as 40% companies staying closed forever once the closed down. The damage from this can be massive for BIT with the fines, regulatory fines. PR mess as most companies get named and shamed now.

Vulnerabilities

Lack of security culture in place that allows for breaches and attacks from occurring easily. Lack of training for staff. Outdated software. A lack of Data Loss Prevention Software (DLP).

Countermeasure

The countermeasure we can put in place to prevent these types of attacks is by training staff, up to date policies with regards to data. Making sure a DLP software in in place. Constant back up.

Prioritization

It is important to prioritize the different types of threats that an enterprise is vulnerable to in order to achieve a good security culture within an enterprise. This will also help to determine which part of the company resources and money need to go in order to be up to with the latest threats.

The table below using a ranking of /10 will determine the threat and vulnerability of each threat type with a total calculated at the end.

	Threat	*Vulnerability*	*Total*
Data Breach	8	8	19
Distributed denial of service (DDoS) attack	8	6	15
Malware Attack	6	4	10
Loss of Data	3	8	11
Insider Threats	8	8	19
Unsecured IoT Devices	2	9	11
Phishing Schemes	7	7	14
Cloud cyber security	5	4	9
Cryptojacking	5	5	10
SQL injection Breach	8	7	16

Based on the score the top five threats for BIT are: Data Breach, Distributed denial of service (DDoS) attacks, Phishing Schemes, Insider threats and SQL injection Breach.

Framework

An IT security Framework is vital for an enterprise to be secure and safe from threat. When this is done correctly it will allow the security leader and staff to deal and combat with cyber threats. These are documents will identify the unique scenarios that can prevent an attack from happening and how they enterprise can deal with such situations.

Data Breach

Information security

Purpose

The purpose of this information security is to establish a security culture within the enterprise with the chief in security officer (CISO) and team to create and implement security policies with constant updates and establish relevant security controls with in order to prevent and deal with malicious and non-malicious attacks as well as protecting the enterprises intellectual property and other information assets.

Scope

All policies produced will be affect all BIT staff, contractors, franchisees, visitors, auditors as well as any persons to have access to BIT IT equipment, such as hardware, software or networks and intellectual properly, whether on site or from remote locations.

Policy

The Chief Information Security Officer (CISO) will be tasked to produce and review information technology security policies. These policies will be regularly reviewed and updated to reflect the current and changing threats and vulnerabilities that can affect BIT. The main goal of the policies is to be used as a baseline for any persons having access to intellectual properties of BIT with the ultimate goal of preventing malicious and non-malicious attacks and safeguarding of intellectual properties.

The CISO will be responsible for the training and education of staff in order to make implementations of the policies with security reports created to test and audit the system in place to check for vulnerabilities.

Compliance Requirements

Legislation

Bespoke International Travel (Franchises) Ltd is obliged to abide by all relevant UK and European. The requirement to comply with this legislation shall be devolved to employees and agents of Bespoke International Travel (Franchises) Ltd, who may be held personally accountable for any breaches of information security for which they may be held responsible. Bespoke International Travel (Franchises) Ltd shall comply with all relevant legislation appropriate; this includes but is not limited to:

- Data Protection Act 2018 (GDPR)
- Freedom of Information Act 2000
- Computer Misuse Act 1990

(Heathcote, 2017)

Audit

Audit will have to be performed to access and check if security policies are in place, updated and working. The CISO will ensure that the procedure with the correct evidence and records is then acted upon if required. This will be based upon the audit policy created by the CISO.

Review

Policy shall be reviewed at least annually by the CISO and the security team in place to ensure it is up to date and following the latest threat, vulnerabilities, threats and regulations and make changes and updates if required.

Sub policies

Acceptable Use Policy (AUP)

All people accessing Bespoke International Travel (Franchises) Ltd information system's hardware, network and intellectual properly for the first time must agree to all the practices of the enterprise in order to have access granted. These will have to be reviewed and signed for before an ID and password is granted. This can be carried out either by the Information security department or the Human resources.

Change Management Policy

This policy is there to manage the process of implementing changes that are made within the enterprise. The policy will make the people working at Bespoke International Travel of the changes that have taken place in the IT, hardware and security systems of the enterprise and to avoid knock on affects to the staff and customers of the enterprise.

Access control policy (ACP)

This policy is created to ensure the safeguarding of the enterprise with regards to access and privileges available to the staff and people with access to Bespoke International Travel (Franchises) Ltd IT system and computers. The policy will determine the level of access and security for individuals using the BIT systems with training and systems implemented to avoid breaches and also dealing with departing staff and reducing access.

SQL injection attacks

Patching

Purpose

The purpose of this policy is to provide guidance and security measures in order to prevent vulnerabilities within the enterprise and to prevent attacks such as SQL injection by patching and updates are regularly checked for, reviewed and install to provide the enterprise with the most up to date and secure IT system and infrastructure.

Scope

This policy is used to be applicable by CISO and the security team as well as the database department or any persons that will be in charge of patching and updating the systems on Bespoke International Travel (Franchises) Ltd IT system.

Policy

The policy will deal with patch management. This will ensure that IT systems of Bespoke International Travel (Franchises) Ltd as well as the hardware in use by the staff and franchisees are up to date with the latest patches. This practice is in place to prevent the system from vulnerabilities and new attacks that might have found ways to penetrate the outdated system. Patch updates should be carried out at regular intervals. They should be tested before installations in order to check for compatibility and comply with the current system in order to prevent system crashes or errors and intellectual loss/damage.

Bespoke International Travel (Franchises) Ltd shall comply with requirements in this policy in order to ensure the safeguarding and security of Bespoke International Travel (Franchises) Ltd, data, assets that the enterprise in possession of. These will include of all IT infrastructure such as desktop PC's, Mac's, routers, servers, switches etc. In circumstances where this is not complied to and an exception is in place, this Shall be documented and forwarded to the management of Bespoke International Travel (Franchises) Ltd.

Compliance Requirements

Monitoring and reporting

Each path and update will require monitoring for performance and vulnerability issues by the security and system management team and reports shall be produced for safeguarding. This will also be used to access the security levels of Bespoke International Travel (Franchises) Ltd. The reports shall be made available for the security and internal audit team.

Audit

Bespoke International Travel (Franchises) Ltd's internal audit team will conduct random assessments to check the enterprise follows the policy and to ensure threats and vulnerabilities are dealt with. If Bespoke International Travel (Franchises) Ltd is found in violation of said policy, corrective procedures shall take place.

Sub policies

IT password Policy

Policy to ensure password created by Bespoke International Travel (Franchises) Ltd staff and all users of IT systems shall adhere to the rules set out by the CISO to ensure the enterprise is safe from threats and vulnerabilities. All users must create a safe and complex password that that contain a minimum of 10 characters with one upper case latter (A-Z) and one number (0-9) as well as characters (@). Passwords should not include personal details such as names, D.O.B and locations of birth as this can lead vulnerabilities in the system.

Limiting privilege

This policy will ensure that administrators and staff with access to the SQL servers are protected towards attackers not vulnerable to attacks as a SQL server administrator that use accounts with root access can make it easier for attackers to gain access to the whole IT system. Therefore, this policy should review all staff and what level of privilege that they should have.

Distributed denial of service (DDoS) attacks

Software Security

Purpose

This policy will provide guidance and security measure for Bespoke International Travel (Franchises) Ltd, CISO and security team with regards software security and how to protect the enterprise from threats and vulnerabilities.

Scope

This policy will be applied to the CISO, security team, networking team and any member of staff from BIT or contractors that also has access to the network and IT systems. Any security subcontractors will also have to deal with this.

Policy

This policy will provide guidance and security measure for Bespoke International Travel (Franchises) Ltd to ensure the software used by the enterprise is securely configured to ensure the enterprise is protected at all times and safe from threats and vulnerabilities and instruction attacks.

- All software used by Bespoke International Travel (Franchises) Ltd shall have be configures securely.
- An Software Configure Record (SCR) shall be in place by the security team to keep a record and maintain the inventory of all the authorised software's used bv Bespoke International Travel (Franchises) Ltd. The SCR record will be used to manage security updates, patches and

configurations. The details that require recording are names, vendors, serial numbers, versions as well as the dates the updates were made available and installed on the system.

- Bespoke International Travel (Franchises) Ltd shall only deal with authorised software vendors.
- Bespoke International Travel (Franchises) Ltd shall make sure no modifications are made to the software's in order to receive full support from software vendors.
- Bespoke International Travel (Franchises) Ltd shall make sure all desktops, laptops, mobile phones and tablets shall have software installed to prevent from unauthorised downloads of software's that can compromise systems and lead system vulnerabilities.

Compliance Requirements

Monitoring and reporting

Monitoring of the Software Configure Record (SCR) should happen regularly to make sure all the software's running on BIT is safe and secure, this record should be made available to the internal security audit team to make sure the security team and the enterprise is not compromised.

Audit

Bespoke International Travel (Franchises) Ltd's internal audit team will conduct random assessments to check the enterprise follows the policy and to ensure threats and vulnerabilities are dealt with. If Bespoke International Travel (Franchises) Ltd is found in violation of said policy, corrective procedures shall take place.

An external audit should also be in place annually to make sure the internal audit team is following the correct procedures.

Sub policies

Recognising abnormality

In order to prevent attacks such as Distributed denial of service (DDoS) and other malicious attacks, employers should receive training to spot any anomalies in the server and network activity, at rare times when the software security or IDS fails, suspicious levels of traffic at abnormal times can mean at attack. A procedure should be in place for the employer to quickly alert the appropriate people and within the security team.

Network monitoring

Regular network monitoring should be carried out by the security team to observer patterns, graphs and trends from ongoing network traffic. These can be used to study in order to identify trends which can make it easier to spot and prevent oncoming attacks. This will also provide the security team of valuable information of an attacker such as IP address etc.

Overprovide Bandwidth

This policy is to be used as a precaution measure to secure Bespoke International Travel (Franchises) Ltd's from non-malicious DDoS attacks. The enterprise should overprovide bandwidth in order to prevent high traffic from busy periods. These can be due to a number of reasons but considering BIT is dealing with holiday deals, this should do before holiday seasons. This will also help with malicious DDoS attacks as the system will have a small window of opportunity to deal with attacks before the bandwidth has ran out.

Phishing Schemes

Education awareness

Purpose

This policy is to provide guidance in line with the private sector policies to provide education awareness for the employers and franchises that have access to Bespoke International Travel (Franchises) Ltd IT systems to educate and create awareness in order to prevent attacks and put in place security measure that ensure Bespoke International Travel (Franchises) Ltd has an security culture in place that complies with the rules and regulations.

Scope

This policy is applied to all members of Bespoke International Travel (Franchises) Ltd, 3rd party contractors and franchises.

Policy

This policy shall ensure that all at Bespoke International Travel (Franchises) Ltd using Bespoke International Travel (Franchises) Ltd IT systems have been made aware and trained of the practices and requirements needed with the IT systems as well as the safe guarding of data and intellectual property. This is required to create an tight security culture within the company from top to bottom in order to make employers aware of tactics used by attackers, these tactics can include phishing scheme, social engineering etc.. to obtain company property etc.

- All Bespoke International Travel (Franchises) Ltd users of the IT systems shall receive security awareness briefing at least annually, these briefings can done via talks, videos etc.
- Users shall be made aware of the consequences of attack on BIT and the benefits the awareness training does.
- How to follow security procedures and protocols
- Stay vigilant and updated with the latest threats and vulnerabilities.
- Comply with rules and regulations set by the appropriate bodies that BIT has to comply with.
- Only authorised users have privileges to access certain information.
- Users will be monitored, and any breach will result in disciplinary hearings.
- Users must pass tests to ensure the training has observed and learnt.

Compliance Requirements

Monitoring and reporting

Reports shall be kept on all staff that have received education awareness training. This is for the auditors and security team to determine that employers have up to date training as well as record for internal and external audits. Any employers that with missing or incomplete records shall get reported to the relevant person to review any wrong doings.

Legal requirements

Whist training users shall be made aware of the fundamental and legal requirements they should adhere to whilst working at/for at Bespoke International Travel (Franchises) Ltd in order to avoid legal issues and fines. The following:

- Data protection Act 2018
- Computer misuse act 1990
- Human rights act 1998
- Freedom of information act 2000
- Copyright, Designs and patterns act 1998 (Heathcote, 2017)

Sub policies

Multi-factor authentication

This policy will be in place at Bespoke International Travel (Franchises) Ltd to create strong multi factor authentications for users with access to Bespoke International Travel (Franchises) Ltd IT systems, data base and applications with sensitive data that can fall under the wrong hands. This policy will ensure the enterprise will not be vulnerable from the varies types of attacks such as phishing schemes therefore when users log into systems such as database they will have to go through a two phase authentication system where a security code will be sent to the user via a safe and secure means.

Data encryption

This policy is to ensure that all sensitive data on Bespoke International Travel (Franchises) Ltd IT systems including 3rd parties working on behalf or for Bespoke International Travel (Franchises) Ltd to be encrypted to avoid being viewed in the event of loss, theft interception by attackers. Bespoke International Travel (Franchises) Ltd should consider the following types of encryption: Boot disk encryption, email encryption, external device encryption, file encryption, folder encryption, mobile device encryption and transport level encryption to minimize all risks of sensitive data being stolen and misused in the event of an phishing attack. (Northwestern University, 2013)

Insider threats

Bring Your Own Device (BYOD)

Purpose

This policy is to provide guidance for Bespoke International Travel (Franchises) Ltd to ensure that they meet the relevant security controls to keep the enterprise safe from threats and vulnerabilities.

Scope

CISO, security team, IT department and all at Bespoke International Travel (Franchises) Ltd with Bring your own device.

Policy

Users operating own devices are required to follow Bespoke International Travel (Franchises) Ltd acceptance user policy. A number of precautions and criteria must be set in place for the devices to prevent attacks occurring such as passwords protection, security software, firewall, antivirus, regular and up to date updates etc.

The devices should also be configured to disable software and code tampering. The enterprise should also keep logs for all the devices with reports regarding software's and updates, BYOD shall be configured to allow for remote access from the IT department in order for troubleshooting as well as safety as to when a remote wipe is required.
All data shall be password protected with strong passwords following the guidance set by the password policy.

Cloud data storage shall be disabled on devices to protect data.

Bespoke International Travel (Franchises) Ltd should consider the use of Mobile Device Management system (MDM) to ensure the safe use of devices.

Compliance Requirements

Incident Response

Bespoke International Travel (Franchises) Ltd BYOD users shall report any incidents with to their device to the IT department.

A log of all incidents shall be kept by Bespoke International Travel (Franchises) Ltd for any investigations required.

Sub policies

Social Media

With the increased use of social media amongst the population, a social media policy needs to be in place to keep BIT safe from malicious, non-malicious threats as well as PR issues that could come by the sharing of sensitive information on these platforms.

This policy shall make staff sign agreements before employment to adhere to a set of rules set by the enterprise. The enterprise shall make it clear if any social media activity can be taken place during work hours and on Bespoke International Travel (Franchises) Ltd property. The use of social media using BIT devices should be forbidden. Social media activity on personal accounts should avoid discussing any BIT related information as well as posting any images and photographs taken on BIT property in order to avoid any sensitive background information from reaching the wrong hands. The enterprise could apply stricter policies with regards to the employers personal posting to avoid being associated with the wrong people. (Heatcote, 2017)

Removable media

This policy is in place to avoid the enterprise from any malicious and non-malicious attacks from removable media. Removable media can be classified as a number of items such as: removable USB drives, external Hard Drives, CD's, DVD's, MP3/4 players, media card readers, SD cards, Digital cameras etc.

Hardware shall be modified to prohibit from these devices connecting to Bespoke International Travel (Franchises) Ltd IT systems unless authorised by higher ups otherwise devices should be scanned for viruses and malware to avoid infection and attacks on BIT IT systems and intellectual property. Company supplied removable media shall pass safety and security checks and if possible, should be password enable with encryption. The enterprise should keep a log of all company issued removable media for audits and investigations. A procedure should also be in place of disposing of removable media and the content to avoid data and information from leaking. (Heatcote, 2017)

Standards, Guidelines

Like any business operating from the United Kingdom and European Union Bespoke International Travel (Franchises) Ltd must follow a number of standards and guidelines that have been set out by a number of regulatory bodies in order to

Data protection act 2018

The Data protection act 2018 controls how your personal information is used by organisations, businesses and government (GOV.UK, 2019)

The Data protection Act is a law that is government by the Information Commissioner's Office (ICO), this is the body that is responsible for enforcing the act in the United Kingdom. The ICO has the power to hand out major fines as well as handing out prison sentences and for that reason it is extremely important for BIT to follow the strict guidelines set by the Data Protection Act.

BIT will have to register with the ICO in order to be allowed to handle personal data. This thus makes BIT a “data controller”. The annual registration fee for BIT will be £35 at the start and when the enterprise does increase in size and revenue it will increase to £500.
Once registrations has been completed and BIT is officially a “data controller”. In 2018 the Data Protection Act was updated to incorporate the General Data Protection Regulation (GDPR) from the European Union with the United Kingdom deciding to use the Data Protection Act to slightly modify and enforce the GDPA.

General Data Protection Regulation (GDPR)

For BIT to comply with the DPA they must also comply with the General Data Protection Regulation (GDPR) according to the ICO. GDPR is a regulation set by the European Union on privacy and data law and is enforced within the European Union states and European Economic Area’s. Although the regulation came into force after the Brexit vote however the United Kingdom decided to be introduced this with some minor changes as enforced this as the Data Protection Act 2018. This replaced the 1998 Data Protection Act.

As BIT will be collecting and storing customers personal data it is extremely important for all people within the enterprise to be educated and tested on GDPR to avoid fines and prosecution as well as bad PR that could bring the end to the enterprise.

One aspect of GDPR that BIT will not have to worry about is the storing of sensitive information, this is regarded as religious view, political, sexual orientation and genetic information as BIT is simply dealing with customers personal information in order to book destinations and holiday. (Burgess, 2019)

“There are eight rights for individuals. These include allowing people to have easier access to the data companies hold about them, a new fines regime and a clear responsibility for organisations to obtain the consent of people they collect information about.” (Burgess, 2019)

As the enterprise grows a number of matters need to be considered to be within the GDPR guidelines. When the enterprise grows to over 250 employers, documentation needs to be in place describing why BIT is collecting data, how they are collecting it and the processing method. Documents stating how long the information is being kept for as well the security measures in place protecting the data. With the monitoring system in place and processing of large amounts of data when the enterprise grows, a Data Protection Officer (DPO) with a team must be employed to comply with GDPR.

If and when a breach does occur, the ICO has to be notified within 72 hours with the people the breach has affected being informed.

The implementation of GDPR will be much easier for BIT as this is a startup enterprise and they have not had to deal with the old DPA which gave consumer less power with their data, such as requesting for their data or asking to get their data erased.

The full regulation 88 pages regulation can be accessed via ec.europa.eu but a starter pack on the ICO website can be beneficial for the company director as well as the CISO, security team to read.

PCI Compliance

As this enterprise will be accepting card payments either through a website or in person via the franchises who meet people to sell their holidays therefore the enterprise needs to compliant with Payment Card Industry Data Security Standard.

This standard makes sure that you are exercising the right controls surrounding the storing, transmission and processing of card holder's details, so that their data is protected. (Litter, 2018)

This will be a mandatory requirement for Bespoke and it will have to prove that the enterprise is compliant, otherwise monthly charges are applied by PCI. There will be a two months' time limit from the time of the enterprises signs a contract with a card payment provider before fines are applied.

A level 1 level of compliance is recommended for BIT due to the number of predicted card payments.

To comply the enterprise will need to act on the following 12 checklists:

1. Install and maintain a firewall configuration to protect cardholder data.
2. Don't use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.
5. Protect all systems against malware and regularly update antivirus software or programs.
6. Develop and maintain secure systems and applications.
7. Restrict access to cardholder data by business need to know.
8. Identify and authenticate access to system components.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security for all personnel. (Litter, 2018)

Once these have been met it's the CISO or personal from the security team to answer a questionnaire to obtain the PCI DSS certificate. As this questionnaire contains many questions and could take a long time a 3rd party contractor could be employed to make sure the enterprise in compliant and gets the certificate. This will need to be updated yearly.

ISO/IEC 27001

Adopting ISO/IEC 27001 for BIT would be highly recommended for a number of reasons that could elevate the enterprise especially with public trust, company image as well help with the aspirations of the enterprise globally.

ISO27001 is an international standard recognized globally for organizations to adapt an information security management system (Singh, 2017)

Information security management system (ISMS) ensures many of the practices recommended in this report, policies and procedures are in place whist confirming that the enterprise is actively following them thus increasing the business profile and trust with customers.

In order, be certificated an audit must be carried out to ensure the enterprise has the security measures in place and will make the enterprise much more attractive in terms of security and peace of mine, especially to the global market and this type of standard international.

Secure Sockets Layer (SSL)

SSL Certificates are small data files that digitally bind a cryptographic key to an organization's details. When installed on a web server, it activates the padlock and the https protocol and allows secure connections from a web server to a browser. Typically, SSL is used to secure credit card transactions, data transfer and logins, and more recently is becoming the norm when securing browsing of social media sites. (Kloepfer, 2019)

This especially in 2019 has become extremely important for websites as browsers have increasingly made aware to consumers that a website that does not have an SSL certificate is "not secure". This is vital for BIT due it being a startup and not being known to consumers and for that reason making sure the enterprise website is shown as secure to new traffic is important.

Obtaining a certificate is simple and can be done through 3rd party security firms or via the hosting service.

Conclusion

For any startup enterprise it is extremely hard to survive within the first few years of business. In order to eliminate the risk of going bust a number of reports and assessments must be carried out. These reports will be beneficial in the long run and can help develop a Business Continuity Plan that will help the business survive in case of cyberattacks as well as help spending resources in the right areas and help the shareholder instill a correct working culture in the enterprise. It's extremely important that if Bespoke International Travel (Franchises) Ltd wishes to operate as a professional enterprise and continuously grow to review and instill the recommendations made through this report.

According to Symantec solutions "To protect your organization from a cyber-attack, it's important to understand how an attacker goes about stealing sensitive information." And this has been one of the objectives of this report. The top 10 current threats of 2019 have been listed and explained in detail with information regarding how it could affect the enterprise and how we can countermeasure it. Of course, we have to assume that the enterprise as a start-up will have some budgeting issues and for that reason a prioritization has been considered for the top five threats. These threats have been prioritized for a reason such as importance, risk factor, relevance and also the fact that the enterprise will be running franchises.

With these five threats, frameworks and policies with sub policies have been created for the staff and stakeholder to follow. The Policies have been set up in a manner to make it as easy as possible for anyone to read and follow with the relevant people listed. In order for Bespoke International Travel (Franchises) Ltd to have any chance of surviving it's extremely important that these policies are followed and enforced because besides protecting the business interests and the intellectual properties, the enterprise will also have the duty to protect personal and sensitive data of customers using Bespoke International Travel (Franchises) Ltd. Breaches can result in heavy fines, bad PR and possible prison sentences. It also important legal and compliance issues are being met.

The policies included in this report have been designed to keep in date with the current threats and vulnerabilities and ways to prevent and tackle these issues, however it is important for the Chief Information Security Officer (CISO) to review these policies regularly and to make sure they are up to date within the current trends. "security policies can stale over time if they are not actively maintained. At a minimum, security policies should be reviewed yearly and updated as needed" (Dunham, 2018)

A number of standards and guidelines the enterprise needs adhere to have been listed in this report. As mentioned some of these such as the Data protection Act and GDPR must be enforced for the enterprise to operate within the United Kingdom however if the stakeholder wishes to run a business to operate within Europe and then Globally it is then recommended to follow and enforce the latter standards and guidelines. Some of these recommendations will cost the enterprise money and considering the enterprise is at the startup stage these costs too heavy but taking shortcuts can lead into stakeholder having to spend large sums of money to eradicate the issues.

Overall this report has considered a number of factors such as the age, budget and aspirations of Bespoke International Travel (Franchises) Ltd with the view of building a security culture within the enterprise and a high strength security posture that will build the trust of consumers. The report has also made it for BIT to take a holistic approach to security that will determine the enterprise will have enough knowledge of threats and vulnerabilities to prevent future attacks rather than reacting to them after damage has been done.

References

Cybrary. (2019). *SQL Injections and Countermeasures - Cybrary*. [online] Available at: https://www.cybrary.it/0p3n/sql-injections-countermeasures/ [Accessed 13 Apr. 2019].

DI (2019). Phishing And Its Impact On Businesses And Employees. [Blog] *Defense Intelligence*. Available at: https://defintel.com/blog/index.php/2017/02/phishing-and-its-impact-on-businesses-and-employees.html [Accessed 11 Apr. 2019].

Gibson, D. (2015). *Managing risk in information systems, second edition*. Burlington, MA: Jones & Bartlett Learning, p.43.

Lord, N. (2019). *Phishing Attack Prevention: How to Identify & Avoid Phishing Scams in 2019*. [online] Digital Guardian. Available at: https://digitalguardian.com/blog/phishing-attack-prevention-how-identify-avoid-phishing-scams [Accessed 13 Apr. 2019].

Weisman, S. (2019). *What is a DDoS attack?*. [online] Us.norton.com. Available at: https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html [Accessed 11 Apr. 2019].

Hayslip, G. (2019). *9 policies and procedures you need to know about if you're starting a new security program*. [online] CSO Online. Available at: https://www.csoonline.com/article/3263738/9-policies-and-procedures-you-need-to-know-about-if-youre-starting-a-new-security-program.html [Accessed 16 Apr. 2019].

Heathcote, A. (2017). *Information Security*. Example policy. NHS.

Pbworks.com. (2019). *Data Breach Policy*. [online] Available at: https://www.pbworks.com/data-breach-policy.html [Accessed 19 Apr. 2019].

Sullivan, P. (2019). *Insider threat protection: Strategies for enterprises*. [online] SearchSecurity. Available at: https://searchsecurity.techtarget.com/tip/Insider-threat-protection-Strategies-for-enterprises [Accessed 14 Apr. 2019].

Bailey, N. (2014). *IT Password Policy*. KCI.

Duhnam, R. (2019). [online] Linfordco.com. Available at: https://linfordco.com/blog/information-security-policies/ [Accessed 15 Apr. 2019].

European Commission - European Commission. (2019). *Data protection*. [online] Available at: https://ec.europa.eu/info/law/law-topic/data-protection_en [Accessed 15 Apr. 2019].

Globalsign.com. (2019). *What is SSL?*. [online] Available at: https://www.globalsign.com/en/ssl-information-center/what-is-ssl/ [Accessed 3 May 2019].

GOV.UK. (2019). *Data protection*. [online] Available at: https://www.gov.uk/data-protection [Accessed 15 Apr. 2019].

Iittler, V. (2019). *What is PCI Compliance and why is it important?*. [online] Payzone UK. Available at: https://www.payzone.co.uk/blog/product-information/what-is-pci-compliance/ [Accessed 18 Apr. 2019].

IoT For All. (2019). *The 5 Worst Examples of IoT Hacking and Vulnerabilities in Recorded History | IoT For All*. [online] Available at: https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/ [Accessed 15 Apr. 2019].

Kloepfer, D. (2019). *What is an SSL Certificate?*. [online] Globalsign.com. Available at: https://www.globalsign.com/en/ssl-information-center/what-is-an-ssl-certificate/ [Accessed 18 Apr. 2019].

Sheridan, K. (2019). *Enterprise Malware Detections Up 79% as Attackers Refocus*. [online] Dark Reading. Available at: https://www.darkreading.com/attacks-breaches/enterprise-malware-detections-up-79--as-attackers-refocus/d/d-id/1333705 [Accessed 18 Apr. 2019].

Singh, A. (2019). *Why Adopting ISO 27001 is Good for Business and Customers*. [online] Cm-alliance.com. Available at: https://www.cm-alliance.com/news/why-adopting-iso-27001-is-good-for-business-and-customers [Accessed 18 Apr. 2019].

Symantec (2013). *Preparing for Cyberattack*. [online] Symantec. Available at: https://www.symantec.com/content/en/us/enterprise/other_resources/b-preparing-for-a-cyber-attack-interactive-SYM285k_050913.pdf [Accessed 15 Apr. 2019].

Bisson, D. (2016). 10 IT Security Risks Your Employees Bring to Your Organization. [online] Available at: https://www.metacompliance.com/blog/10-it-security-risks-your-employees-bring-to-your-organization/ [Accessed 12 Apr. 2019].

Bradley, A. (2018). Crytojacking 101; why cryptojacking is bad for business -. [online] Enterprise Times. Available at: https://www.enterprisetimes.co.uk/2018/10/24/crytojacking-101-why-cryptojacking-is-bad-for-business/ [Accessed 10 Apr. 2019].

Consolidated Technologies, Inc. (2018). Data Loss: Causes of it, Effects on Businesses & How to Prevent. [online] Available at: https://consoltech.com/blog/10-common-causes-of-data-loss/ [Accessed 15 Apr. 2019].

Enterprise Security News | Endpoint Protection Solutions Blog | Comodo. (2019). What is Data Loss Prevention? | Why DLP and How DLP Software Works?. [online] Available at: https://enterprise.comodo.com/blog/data-loss-prevention-software/ [Accessed 18 Apr. 2019].

ESG 2015. (2015). andards and Guidelines for Quality Assurance in the European Higher Education Area.
Heathcote, A. (2017). Education Awareness. Policy Example. NHS England.

Heathcote, A. (2017). Removable Media. Example Policy. NHS England.

Heathcote, A. (2017). Social media. Example policy. NHS England.

It.northwestern.edu. (2018). Information Security Policy and Standards: Data Encryption: Information Technology - Northwestern University. [online] Available at: https://www.it.northwestern.edu/policies/dataencryption.html [Accessed 14 Apr. 2019].

Lord, N. (2019). Phishing Attack Prevention: How to Identify & Avoid Phishing Scams in 2019. [online] Digital Guardian. Available at: https://digitalguardian.com/blog/phishing-attack-prevention-how-identify-avoid-phishing-scams [Accessed 12 Apr. 2019].

Nadeau, M. (2018). What is cryptojacking? How to prevent, detect, and recover from it. [online] CSO Online. Available at: https://www.csoonline.com/article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html [Accessed 18 Apr. 2019].

NHS (2017). Bring Your Own Device Security. Example Policy. NHS England.

NHS (2017). Patching. Example policy. NHS: NHS England.

The Security Ledger. (2018). Survey: Attacks Find Insecure IoT Devices. [online] Available at: https://securityledger.com/2018/11/survey-finds-attacks-find-insecure-iot-devices/ [Accessed 3 Apr. 2019].

Zorz, Z. (2019). How are businesses facing the cybersecurity challenges of increasing cloud adoption? - Help Net Security. [online] Help Net Security. Available at: https://www.helpnetsecurity.com/2019/02/21/enterprise-cloud-adoption-security/ [Accessed 10 Apr. 2019].

Anon, (2017). *Phishing And Its Impact On Businesses And Employees*. [online] Available at: https://defintel.com/blog/index.php/2017/02/phishing-and-its-impact-on-businesses-and-employees.html [Accessed 8 Apr. 2019].

Kingori, D. (2019). *Top 10 Cybersecurity Risks For 2019 | United States Cybersecurity Magazine*. [online] United States Cybersecurity Magazine. Available at: https://www.uscybersecurity.net/risks-2019/ [Accessed 5 Apr. 2019].

SearchSecurity. (2019). *Crafting an insider threat program: Why and how*. [online] Available at: https://searchsecurity.techtarget.com/ehandbook/Crafting-an-insider-threat-program-Why-and-how [Accessed 3 Apr. 2019].