Cyber Security Whitepaper

☎ 08000 122 225
✉ info@tribeca-it.com
www.tribeca-it.com
16 Berkeley Street, London, W1J 8DZ

Tribeca
TECHNOLOGY GROUP

Contents

Introduction

You have no doubt heard the term Cyber Security. It is fast becoming a hot topic in most organisations. This document has been written to provide an insight into Cyber Security and outline some best practices in the modern Enterprise.

Why is Cyber Security Important?

With high profile organisations being hacked, Cyber Security has risen to the top of the World's economic agenda. With the increasingly networked world we live in, an organisations Cyber Security regime not only affects them but everyone around them. From a personal Facebook account being opened at work, to a company email being sent to another organisation. The modern world is networked and Cyber Security affects everyone.

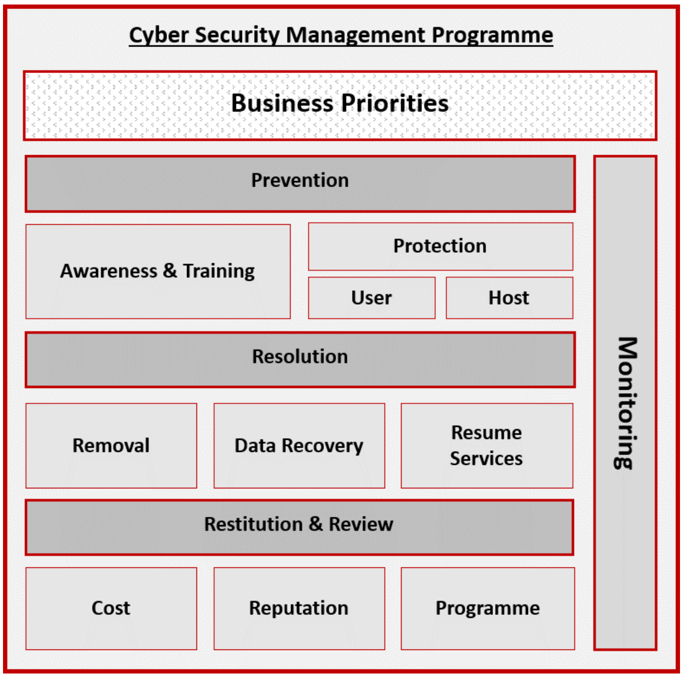
Cyber infections easily multiply. It takes only one account to be compromised for an attack to spread out and infect anything associated to it. The infection exists already and is only growing. Now is the time to think about Cyber Security and how best to protect your business.

According to an independent UK Government survey conducted by PWC in 2015, security breaches have been on the rise. **90%** of large organisations and **74%** of small businesses suffered from at least one security breach. The scariest finding is the cost to UK businesses. The average cost of the worst breach for a large organisation is between **£1.46 million** and **£3.14 million**. Small businesses suffered an average loss of between **£75k** and **£311k**. This is almost double the findings in 2014. The results of the survey can be found on the PWC website - **www.pwc.co.uk**

Cyber Security Management Programme

Tribeca suggest that every organisation should have a Cyber Security Management Programme in place to help reduce the overall cost of security breaches. Modern threats are continuously evolving every second forcing the requirement for more enhanced security measures. A management programme will provide the best protection and steps for resolution and restitution. It is just as important to plan for breaches and minimise the impact as it is to prevent them. **Apple**, **Sony** and **Google** are three of the largest corporations to be infiltrated. They already had plans in place to minimise the impact and recover their brands reputation.

Below is a diagram showing the different aspects of a good Cyber Security Management Programme. The programme is based around three key stages; Prevention, Resolution and Restitution & Review, all controlled by Business Priorities.



Cyber Security Management Programme

Business Priorities

Prevention

Awareness & Training

Protection

User

Host

Resolution

Removal

Data Recovery

Resume Services

Restitution & Review

Cost

Reputation

Programme

Monitoring

Business Priorities

Priorities are different for every organisation, depending on what is important to maintain the business. Tribeca understand that your Cyber Security Management Programme needs to be tailored to your affordability and business continuity requirements.

It is important to understand what is critical to the business, what loss of function would have the greatest cost implications. Consider data loss, information in the wrong hands, brand reputation, loss of communication, staff not being able to carry out certain tasks etc. All of this information needs to be communicated to whoever produces the programme. Knowing what is important to the business is key to planning the best protection.

Monitoring

Monitoring should be carried out at all times in one form or another. There are different forms of monitoring that can be carried out to ensure security is kept to an agreed standard.

Real-time Reporting

This can be useful to determine if machines or services are not secure. Potential security holes can be detected and plugged before any harm is done. Below are some examples which could be implemented.

- **AV/Malware Central Management** – This provides a central management point for protected hosts, allowing them to report on whether or not they have the most current Virus/Malware definitions. It also allows hosts to report on other potential security risks, such as dangerous software etc.
- **Firewall Alerts** – Some firewalls can be configured to send out alerts when suspicious activity occurs.
- **System Monitoring** – There are monitoring tools which can monitor your network and services for potential risks, such as old encryption algorithms, open ports or missing security patches.

Penetration Testing

There are companies that specialise in testing your networks security. They can carry out risk free, up to date attacks which reveal any potential flaws. Also, they usually offer advice on how to resolve the issues found.

Vendor Subscriptions

Vendors usually alert their customers about security updates via email. Sometimes subscribing to their mailing list or support program will allow you to receive alerts on any security issues they have found. It is not uncommon for patches to be produced but not publicised.

Regular Assessment of the Programme

There are a lot of variables within the Cyber Security Management Programme, so it should be assessed regularly, regardless of whether or not breaches have occurred. Business Priorities can change along with the availability and quality of resources.

Prevention

The prevention step is arguably the most important and focuses on stopping cyber breaches in their tracks. This should be robust enough to account for any eventuality, however the business priorities may well require some elements to be resized or even excluded completely.

Awareness & Training

A study carried out by ESET (one of the top Cyber Security solutions providers) revealed that **90%** of consumers have not had any Cyber Security training in the last 12 months and **68%** have had no training at all. That could translate to **68%** of your staff being unaware of suspicious behaviour, dangerous websites, infected emails and much more.

With almost **100%** of the UK and US workforce having access to an Internet capable device, they are more likely to be the first to come across a potential threat, whether it be a pop up on a website or an email with a virus attached. Staff awareness is often overlooked but it is one of the most important steps in preventing breaches before they happen. Tribeca can offer guidance on how to raise awareness within your organisation.

Protection

Pretty much all organisations employ some form of protection already. However, there is much more to it than having a firewall and an Anti-Virus program.

User

The majority of User constraints are created within the business and are focused around written guidelines and restrictions; a set of cyber related rules and regulations your organisation has in place for anyone that comes in to contact with the business. This could simply be incorporated into the company handbook or it could be a set of separate company polices. Written company policies should come from within the organisation, however below are some of the things that should be considered.

- **Physical Access** – Security should be in place to prevent unauthorised access to core equipment. Security passes and locks should be in place where possible. There should also be a controlled distribution and record of passes and fobs etc.
- **Data Mobility** – *What are the rules around sharing data and taking it outside of the organisation?* This should be communicated to the staff so there is a clear understanding. Tribeca could also implement perimeter restrictions, preventing users from uploading or downloading data with certain heuristics.
- **Internet Usage** – Consider the rules and regulations around Internet usage within the organisation. Tribeca can also implement restrictions on browsing, preventing access to certain sites according to category or white/blacklists.
- **Device Usage** – *What is acceptable usage of desktop PC's, Laptops and mobile devices?* Management software could be implemented to monitor and control usage of these devices.
- **Remote Working** – *Do you require any restrictions for remote workers?* You should consider acceptable work places and devices. For example; *is it acceptable for a user to connect to the network via an unmonitored PC in an unsecure location?*
- **Privileged Account Access –** It should be clear who has access to Privileged accounts. A list or register of people with privileged access may need to be kept.

- **Password Policy –** Forcing users to have complex passwords and to change them regularly helps prevent accounts being compromised. A hacked account could give a hacker access to your entire network.
- **Representation** – Staff should be made aware of what is acceptable to say or share about your business outside of work. It may or may not be acceptable to say certain things which could affect the company's reputation. A harmless post on Facebook could spread and grow into much more.
- **SOP's** – Standard Operating Procedures outline exactly how certain tasks should be carried out. For example, an SOP for the Leaver process can ensure that all the correct steps are carried out, reducing the risk of a user maintaining access or keeping devices they shouldn't have, once they have left the organisation.
- **Forms** – A form should be used where possible, when requesting regular changes, such as New User or a Leaver. Forms provide specifics and allow you to control exactly what actions are taken.
- **Sign-Off Authorities** - Agreed sign-off authorities can prevent unauthorised activity within your organisation. The number of authorities should be kept to a minimum.
- **File Access** – Decide how you want to restrict access to files as this can affect how your file structure is organised. For example you could have a folder for each department and security permissions could be based upon department members. Communicate the restriction requirements to Tribeca so we can maintain them.
- **Asset Management** – Registers may need to be kept of all the company's property. This could be physical property such as laptops and mobile phones, or it may include intellectual property. Who has been issued what document and when. These registers may become key in recovering from a security breach.

There is a lot to consider but most of the above is probably already in place in one form or another, such as contract statements relating to intellectual data or an Internet Usage Policy. You should think about how restrictive you want to be. It is fair to say that in some cases, too much red tape can be counterproductive. That is why the Business Priorities should be used to tailor the User constraints.

Host

Host protection relates to devices within your organisation such as PC's, mobile phones and Servers. This may be inside or outside the corporate network, although protection outside the network is much harder to manage due to the reduced level of control. There is likely to be some overlap with the user constraints. For example, polices on acceptable device usage may also outline what software can and cannot be installed onto a PC.

- **Perimeter Security** – This is the first physical line of defence. It is placed on the edge of the network and stops threats before they can infiltrate your organisation. They can also prevent threats from leaving your organisation, protecting your reputation.
  - **Firewall** – These come in many different variations, offering different layers of security and control. Modern firewalls not only carry out port blocking but can also provide AV scanning, SPAM Filtering, Intrusion Prevention Systems, Data Loss Prevention, Application Control and much more.
  - **Email Washing** – Email can be configured to flow through a perimeter service and malicious items be removed. The service can also prevent malicious and SPAM emails from ever being sent using certain characteristic checks on the sender.
  - **IPS** – An Intrusion Prevention System can be implemented at the perimeter to help protect against malicious network flow attacks such as Distributed Denial of Service (DDoS).
  - **Application Control** – Offers the capability of identifying and blocking potentially unsafe or unwanted applications according to certain characteristics.
  - **VPN** – Where possible, secure VPN's should be used when linking different networks, whether it be another office or a user's home network. These will ensure data transferred between the networks is encrypted and protected against theft or manipulation.
- **Anti-Virus** – AV Software has common place within pretty much all organisations now. It can protect against most infections and is usually focused upon scanning files for certain signatures. There are many things to consider when implementing AV software. Tribeca can help you choose the correct software and decide on how it is best implemented. Regular or on access scanning, infection control and instant reporting are some of the things that should be considered.
- **Anti-Malware** – Malware is a term used to describe any malicious software, but is usually focused around Adware and Spyware (continuously changing malicious software that tricks the end user into downloading it, usually via internet browsing or installing software). It is often assumed that AV software will also protect against Malware. That may be the case with some AV software but it is becoming more apparent that Malware focused software can offer better protection.
- **Patch Management** – With some of the biggest security breaches of the last few years taking advantage of old software bugs, it has become more apparent to vendors that patching their software is top priority. You should consider whether or not these patches should be applied within your organisation. All software should be treated individually as the patch work may result in a different level of disruption to the business. Tribeca can provide schedules and carry out patch work with as little disruption as possible.
- **Encryption –** Drive encryption can protect data on a device that has fallen into the wrong hands, making it inaccessible. It also has a performance impact which should be considered.

- **Removable Storage** - You may want to enforce removable storage restrictions which will not only help prevent data theft but also protect devices from infection or damage.
- **Screen Lock -** Forcing the screen to lock on a PC or mobile device after a few minutes can help prevent unauthorised access.
- **Mobile Device Management –** MDM software can provide some control over user's devices when they are outside of the network. It provides features such as wiping a lost device or forcing a PIN requirement. This is increasingly important with the use of Smart Phones and Tablets within the workplace. Restrictions can be tailored to each user as required.
- **Following Guidelines –** Following the correct guidelines when installing and maintaining software and hardware is important to ensure it is protected correctly.

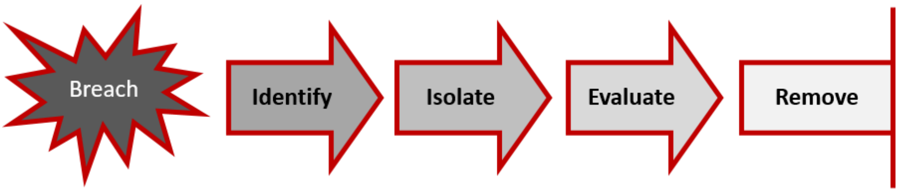
Resolution

Although Cyber Security is fast evolving, a breach is still a risk that could damage to your business. Advanced planning for these breaches can mitigate the damage.

With your IT Services outsourced to Tribeca, we can use tried and tested processes we already have in place. However, there may be some requirements for you to consider. For instance, if a virus damages your company data, a sufficient backup of that data may be required to achieve a full resolution.

Removal

Resolution only starts if a threat enters your network and becomes a risk. Once it does, the removal process should start. Below is a high level outline of the process.



1. **Identify** - The first stage is identification, what has happened or what virus is it etc.
2. **Isolate** – The risk should then be isolated so it does not spread.
3. **Evaluate** - The next stage is to evaluate the risk and determine the steps to follow.
4. **Remove** – The risk is then removed.

Recovery

The next stage is to recover anything that has been directly affected. Some examples shown below.

- **Data** – Lost or damaged data could be recovered if there are suitable backups in place. An acceptable Recovery Point Objective should be agreed with your backup provider. More recovery points provide a larger recovery window but will also require more storage and add to backup costs, however, less recovery points may result in more data loss and older data being recovered. Choosing the right backup solution and implementing it to suit your Business Requirements is very important and something Tribeca have experience with.
- **Workstations** – When a workstation has been compromised, it may need to be recovered. After the level of damaged has been assessed, Tribeca's experienced engineers can recover the workstation with as little disruption as possible. Having spare workstations and a good software inventory help improve recovery times.
- **Services** – Services such as email, remote access or web browsing could be disrupted. Issues should be resolved to recover these services as soon as possible. Again, Tribeca's experienced engineering team can bring services back online as soon as possible. In a virtual environment, keeping copies of entire servers can drastically reduce recovery times. A Disaster Recovery environment may already offer some form of recovery for individual servers.

Resume Services

Services should be resumed once a breach has been dealt with. For example, once a PC has been rid of a virus, a user can continue to use it straight away. However it may have spread by email and therefore, email services may have been disabled as part of the isolation process. Procedures should be in place, detailing how to resume services and access to the relevant accounts should be provided to Tribeca or internal IT staff dealing with the breach.

Restitution & Review

Once a breach has been dealt with and services resumed, there may still be some additional work to carry out. A review of the breach may reveal any cost implications which could, for example, be required for insurance purposes. The review could also reveal any impact on the company's reputation. Steps may need to be taken to reinforce the company's brand. All of these things need to be considered.

Finally, a review of the Programme itself and steps carried out, should take place. For example:

- *Can we improve any of the procedures?*
- *Do any of the Policies need to be amended*
- *Do we need to implement different security features?*

This will ensure that security is kept tight and up to date, improving prevention and allowing for fast recovery times.

Action and Review Team

To enable an accurate action and review process a **Computer Security Incident Review Team** (CSIRT) should be implemented, consisting of the following:

- **CSIRT Team Lead**
  - The CSIRT team lead will be responsible for the activities of the CSIRT and will coordinate reviews of its actions.
- **CSIRT deputy Team Lead**
  - Responsible for assuming the role of Team Lead in their absence
- **CSIRT IT Contact**
  - Responsible for communicating between the CSIRT and the IT team, as well as diagnosing and implementing the fix.
- **CSIRT Legal Representative**
  - The Legal Representative determines how to proceed during an incident with minimal legal liability and maximum ability to prosecute offenders
- **CSIRT Communications Officer**
  - Responsible for communicating the incident response to employees and third parties
- **CSIRT Management Representative**
  - Responsible for approving and directing security policy

Summary

Cyber Security should be taken seriously in any organisation as any one breach could potentially cost the company a significant sum. It is important that a good programme is planned and covers, not only how to deal with a security breach, but how to prevent them and what to do once it's been resolved. Tribeca can help assess what elements you already have in place and discuss how best to produce a robust programme which suits the needs of your business.

About Tribeca

For more than 10 years, Tribeca has delivered world-class, specialist IT services to the demanding Alternative Investment market. Our services include Business IT Support, Cyber Security, Disaster Recovery, Network Design, Data Centre Hosting and Software Development.

We now support a wide variety of clients across 15 countries and monitor their infrastructures 24/7/365 with over 9,000 monitor sensors connected. Our team is more than capable of keeping up with your business's fast pace of work and constant need for robust and reliable IT. We will ensure that your systems are working at their optimum level, enabling you to do your job as effectively as possible. We use only the latest high-performance technology to guarantee you the best service. Our instant response helpdesk can resolve over 90% of our clients' issues remotely. This is because our first line engineers are trained to a similar standard as that of other companies' second line teams. This efficiency benefits you by remedying technical issues promptly to minimise any inconvenience to your network.

Tribeca is committed to delivering the best outsourced IT support service within the financial sector. We guarantee to reduce your IT overheads, including third-party providers. As part of our dedicated service, we can assure you that you will always deal with a full-time employee, as we never use calls centres or contractors.

For further information, visit www.tribeca-it.com, email us on info@tribeca-it.com or call us on 08000 122 225