Business Privacy Essentials

This document was created by Stuart W while offering consultancy services to SME businesses to help them improve their security profile. I have now taken an employed role with a global software developer as the Security Policy and Procedure Writer. As such, TechSecScot.com is now being used to help those interested in a future career in Cybersecurity to find the information and training they need to take their first steps up the ladder of success.

This document is being published free of charge to LinkedIn in the hopes that it is shared with people it may help. Cybersecurity is a massive worry to many small business owners throughout the planet and as such, I want to help reach those people and provide easy to understand instructions. It is designed to be used in conjunction with the Gap Analysis document to help businesses prepare for Cyber Essentials certification. Cyber Essentials is a security framework in the UK produced by the National Cyber Security Centre (NCSC) to improve the security of businesses. People reading this document outside of the UK can still use the documents to improve their security profile even though there is no certification available to them.

If you use this document to improve the security profile of your business, please connect with Stuart W on LinkedIn and leave a recommendation to say thanks.

Data Protection Act 2018 (GPPR)

As a business operating within the UK, you are regulated by the DPA 2018 (GDPR) which is the UK equivalent of the EU GDPR legislation. The act states:

Everyone responsible for using personal data has to follow strict rules called "data protection principles." They must make sure the information is:

- *used fairly, lawfully and transparently*
- *used for specified, explicit purposes*
- *used in a way that is adequate, relevant and limited to only what is necessary*
- *accurate and, where necessary, kept up to date*
- *kept for no longer than is necessary*
- *handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage*

What is Personal Data?

The Information Commissioners Office (Responsible for Administration of DPA 2018) State:

Understanding whether you are processing personal data is critical to understanding whether the UK GDPR applies to your activities.

- *Personal data is information that relates to an identified or identifiable individual.*

- *What identifies an individual could be as simple as a name or a number or could include other identifiers such as an IP address or a cookie identifier, or other factors.*
- *If it is possible to identify an individual directly from the information you are processing, then that information may be personal data.*
- *If you cannot directly identify an individual from that information, then you need to consider whether the individual is still identifiable. You should take into account the information you are processing together with all the means reasonably likely to be used by either you or any other person to identify that individual.*
- *Even if an individual is identified or identifiable, directly or indirectly, from the data you are processing, it is not personal data unless it 'relates to' the individual.*
- *When considering whether information 'relates to' an individual, you need to take into account a range of factors, including the content of the information, the purpose or purposes for which you are processing it and the likely impact or effect of that processing on the individual.*
- *It is possible that the same information is personal data for one controller's purposes but is not personal data for the purposes of another controller.*
- *Information which has had identifiers removed or replaced in order to pseudonym-ise the data is still personal data for the purposes of UK GDPR.*
- *Information which is truly anonymous is not covered by the UK GDPR.*
- *If information that seems to relate to a particular individual is inaccurate (i.e. it is factually incorrect or is about a different individual), the information is still personal data, as it relates to that individual.*

What does this mean for my business?

It means that if you are collecting 'Personal Data' of customers, employees, or volunteers then you need to take the 6 Principles stated above into account. Regarding your IT Systems, principles 4 & 6 are the major influence.

The Security of that Personal Data must be one of your highest priorities as a business. The fines for not providing adequate security of customer personal data can be 4% of the Business Global Annual Turnover. In some cases, this goes into the many millions of £'s.

Do not stress too much, there are things we can do to help you protect that data. There is a security framework called Cyber Essentials which helps businesses go about making changes to improve their security profile.

Information Security Policy

As the business owner, you should also write an Information Security Policy which should be made available to your customers and staff. This will show that you are committed to doing the right thing by them and will give them confidence you know what you are doing with their personal data.
TechSecScot can help you with this!

Cyber Essentials

This is a UK Government initiative to help small businesses improve their Cyber Security. Essentially providing some basic advice on security controls, following easy steps to give your business a higher but achievable Security Profile. It was introduced by the National Cyber Security Centre an offshoot of GCHQ. Information on Cyber Essentials can be found here on the NCSC website

The scheme is separated into two parts: Cyber Essentials and Cyber Essentials Plus. The Plus version is much more in depth however as a small business, the entry level version is achievable. It states:

- Use a Firewall to secure your internet connection.
- Choose the most secure settings for your devices and software.
- Control who has access to your data and services
- Protect yourself from Viruses and Malware.
- Keep your devices and software up to date.

I will run through the requirements with my suggestions on how you can make your business comply with them.

Hardware Firewall

A Firewall is a Filter of data packets. It follows a set of rules, which can be changed to allow or disallow various types of traffic. Your Internet Service Providers router may contain a basic firewall, I would encourage you to buy a SOHO Router with inbuilt Firewall to ensure you have adequate protection at the edge of your home/business network.

A dedicated firewall such as a PFsense Firewall is an amazing option to have. It is more expensive but gives you much greater flexibility and services to help secure your network. PFsense sell plug and play devices but they also have the software Open Source on the internet. If you have an old laptop, you can install the software and have an awesome firewall / router for your business. The laptop will require two Ethernet ports, you can buy a USB Ethernet port for a few £'s on Amazon.

Option 1 – SOHO Router with inbuilt Firewall
SOHO Router – Something like this would do the job.

Option 2 – Dedicated Software Firewall with additional Access Point
PFsense Software – Old laptop will need to be wiped clean and this installed as new OS
USB Ethernet Adaptor – Only required if you go for PFsense on old laptop.
Access Point – You will also require a wireless access point with Ethernet ports if you go for the PFsense Firewall. You could use the SOHO Router above for this.

Option 3 – Dedicated Hardware Firewall with additional Access Point
PFsense Hardware – Use the comparison chat to decide best option. You will need an additional WIFI Access point with Ethernet ports if you go with this option. SOHO Router above would work.

Software Firewall for Your Computers

A Software Firewall is a program that you install directly on your computer to protect it from outside interference. It is a packet filter which will allow or deny access to ports on your computer in alignment with the rules set as default or as changed by you. There are many free Software Firewalls but, in this case, I would always recommend paying a few £'s to ensure you are getting the best protection and that your data is not being harvested.

I use BitDefender Internet Security but there are many alternatives. Have a look at this Article where you will find some good options.

Windows Defender is included free with Windows 10 Professional and is a viable option. It's a little clunky but will do the job.

Choose the Most Secure Settings

When computers are built, they are often preconfigured to be quite open to connections and contain lots of software that is not required for business activities. It should be your goal to close unused connections/ports and remove software which is not required.

Closing ports can be done through firewall rules. You will have to set these rules yourself. Uninstalling Programs/Software is done through the Control Panel.

User Accounts

Every user on your work computer should be given a dedicated user account. Try and avoid mixing personal use with work use and if possible, avoid letting family members use the computer you use for work for their entertainment.

You should work on an account that does not have Administrator Privileges and have a dedicated Admin Account for that purpose.

Backups

Data you hold on to for your customers, must be protected from Loss as part of the 6th Principle of the DPA 2018. It is therefore recommended that all protected data is backed up for its security from loss. It is good practice to have three copies of the data, on two different forms of media and one being in a remote location such as the cloud.

Encryption

Personal data that you hold on to of others, is required to be protected as accurate data. This means that we must protect the integrity of that data. A good way of doing this is through encryption. You can encrypt individual files or whole drives. We need to be using encryption when that data is in transit, so with encrypted emails and secure protocols such as https. We also need to secure that data when it is at rest and not being used. Whole drive encryption is a great way to do this. BitLocker is a program that will do this, and it is provided free with Windows Professional products.

Encrypted Email

Some services such as Gmail have the option of encrypting your email. Make sure your email is using port 443 and you can be assured that it is encrypted. Another fantastic option is using an encrypted email service such as **ProtonMail**. They provide a free account, and the service is rather good. There is the option to password protect your emails and auto delete the email from the recipient's inbox after a period. They use an encryption standard called 'Pretty Good Privacy' which is yet to be broken.

Passwords

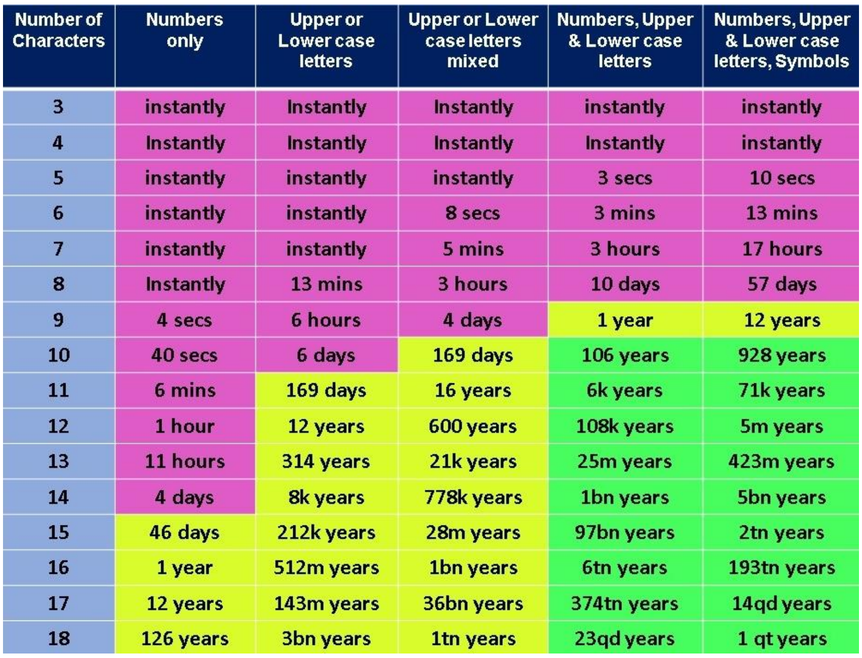
Password cracking is easy using tools available free online. After lists of millions of known passwords were released from a Hacked Database called 'Rock You', it became even easier. For this reason, we need to make our passwords long, complex, and difficult to guess.

Here is a great video on how Passwords are cracked.
Here is a video from the same person on how to make a secure password
Here is a short video if time is a consideration: creating a secure password

A very secure password should contain:

- 20+ Characters
- UPPER and lowercase Characters
- Numbers and Symbols
- No Single Words
- Consider using a phrase or a mix of 4+ Words with Numbers and Symbols
- A less commonly use language such as Latin or Scots would be much harder to crack.
- **NEVER REUSE A PASSWORD**

This table shows how long it takes for computers using cracking tools to break passwords. This can be reduced using very powerful computers, but it gives a good picture of the ease of some.



Number of Characters	Numbers only	Upper or Lower case letters	Upper or Lower case letters mixed	Numbers, Upper & Lower case letters	Numbers, Upper & Lower case letters, Symbols
3	instantly	Instantly	Instantly	instantly	instantly
4	Instantly	Instantly	Instantly	Instantly	instantly
5	instantly	instantly	instantly	3 secs	10 secs
6	instantly	instantly	8 secs	3 mins	13 mins
7	instantly	instantly	5 mins	3 hours	17 hours
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
13	11 hours	314 years	21k years	25m years	423m years
14	4 days	8k years	778k years	1bn years	5bn years
15	46 days	212k years	28m years	97bn years	2tn years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	36bn years	374tn years	14qd years
18	126 years	3bn years	1tn years	23qd years	1 qt years

Default Passwords

Internet Connected Devices such as Routers, Printers, CCTV Cameras and TV's will all come with a default password within the configuration. **The first thing to do with these devices once they are connected is to get into the configuration settings and change the password.** Often these default passwords are well known of or even printed within the manual. Hackers will scan the internet looking for these devices and try the default password to try and get in.

Password Managers

With the number of companies requiring a user account to sign into their websites on the rise; the number of passwords you need to remember can get out of hand very easily. There are a few options available to you. You can write them down, which I would not recommend. If someone gets hold of your password list, they have access to everything. You can store them in a browser or have google store them for you. Again, I would not recommend these options as they are vulnerable if someone gets into your device. What I do recommend is a Secure Password Manager!
There are plus and minus points when it comes to Password Managers such as putting all your eggs in one basket. However, in my opinion the good far outweigh the bad.

A good Password Manager will be:

- Recommended by the Cyber Security Industry
- Passwords stored using 'Salted Hashes' (See video for info of Salted Hashes)
- Encrypted
- Capable of Two Factor Authentication (See Below for full details)
- Free or Inexpensive
- Capable of Generating Passwords with customizable options.
- Integrated with browser extensions or add-on.
- Automatically enters log in or sign on details.
- Capable of syncing between browser and Mobile App
- Integrated with mobile browser through Hardware Settings.

Here is a list of well-known and recommended Password Managers: Article
I use one on this list, however I will let you make up your own mind.
The key thing here is that you have one **'VERY'** secure password that you use to log into the manager, and it does the rest for you.
Enable Two Factor Authentication for the Password Manager and every account that has the option!!!!!!!!!

What is Two Factor Authentication?

It is a security protocol whereas you enter your login details, the service will try and get you to confirm that it is really you trying to log in. They can do this through several means such as Phone Call or Text Message, Using an Authenticator App like 'Authy' or through their own app on your mobile.

It falls into the Authentication principle of 'Something you Have', your Password is 'Something you Know' and if using Biometrics such as facial recognition or fingerprint scan then that is 'Something you are'. Two Factor Authentication requires two forms of input from these three categories.
If you do not provide the requested information, the service will deny you access. It is a very secure way of authenticating the user and it is highly unlikely that a malicious actor will have both forms of authentication. It is not impossible though and we must remain vigilant.

Anti-malware / Anti-Virus

Bit Defender Internet Security comes with Anti-Malware as part of the package. Use it regularly to scan your system, scan documents you have downloaded before you open them and scan USB Drives as they are plugged in. It is a fantastic tool for personal security on up to 3 devices.

If you choose another company, make sure that the Anti-Malware is included in the package and utilise it fully.

Software Updates

While often being a disturbance to your use of a device, Software Updates are imperative to keeping your devices secure. It was not until I learned about Hacking that I truly began to appreciate the little notification in the corner telling me to update.

The updates contain security fixes. Now this does not sound like much until you learn that not updating or patching, the device could potentially be left vulnerable to a hacker bypassing security controls and accessing your system remotely. The updates fix known and published Vulnerabilities that the entire security industry and all the hackers have been made aware of. There are hacking tools that will use the vulnerabilities to take over a computer and then the network.

When you see the ‘Software Update Available’ notification, save your work, click the notification, start the update, and go and put the kettle on.

This goes for all software on your computer, not just the Operating System!

End Of Life Software

As time goes on, companies such as Microsoft will bring out new software. After a few years of bringing out new software, they will stop providing updates for older software. When this happens, newly found vulnerabilities within the old software will not be patched by the manufacturer. This is a massive security risk and can be the reason why so many Hacked Businesses suffer Ransomware and Data Breaches.

If you have EOL Software on your system, you should remove it and purchase software that is supported such as the latest version of Windows.

TechSecScot Services

Stuart is not currently offering consultancy services but please feel free to reach out on LinkedIn for advice. He is normally very happy to signpost you in the correct direction.

Cyber Essentials – Gap Analysis

Company Details

Name_ ______________________________

Company No ______________________________

Address ______________________________

____

____

Postcode ______________________________

Phone No ______________________________

Person Completing Form

Name ______________________________

Email ______________________________

Framework Requirements

- Use a Firewall to secure your internet connection
- Choose the most secure settings for your devices and software
- Control who has access to your data and services
- Protect yourself from Viruses and Malware
- Keep your devices and software up to date

The requirements apply to all the devices and software that are within the Scope boundary and that meet the conditions below:

- *Accept incoming network connections from untrusted Internet-connected hosts*
- *Establish user-initiated outbound connections to arbitrary devices via the Internet*
- *Control the flow of data between any of the above devices and the Internet*

Scope

- Scope Document Complete?
  - Y / N
- TechSecScot ‘Business Privacy Essentials’ Document Complete?
  - Y / N

Policies

- Information Security Policy – Y / N
- Password Policy – Y / N
- Privacy Policy – Y / N
- Acceptable Use Policy – Y / N

Mobile Devices & Bring Your Own Device

- Organisation and BYO Mobile Devices are **IN SCOPE** if accessing Organisation data or services. Are these devices **IN SCOPE**?
        - Y / N
- Are Users allowed to Bring Your Own Device (BYOD)?
        - Y / N
    - If Yes: Is there a BYOD Policy?
        - Y / N
    - If No: Enforcing Strong access policies will help the organisation to protect PII and MDM should be considered.
    - Create BYOD Policy?
        - Y / N
- Is Mobile Device Management used to control devices?
        - Y / N
- Give details

  ____
  ____
  ____
  ____
  ____

- Recommendations:

  ____
  ____
  ____
  ____
  ____

Wireless Devices

- Wireless Devices including Wireless Access Points are **IN SCOPE** if they can communicate with other devices via the internet.
- Does the organisation use Wireless Devices that are **IN SCOPE**?
        - Y / N

    - If Yes: Do devices have adequate protection as per the Cyber Essentials requirements?
        - Y / N
- Recommendations:

  ____
  ____
  ____
  ____
  ____

External Services - Cloud

- Cloud Services such as Data Storage or IaaS are **IN SCOPE**. PaaS and SaaS are **OUT OF SCOPE**
  - Does the organisation use these services?
    - Y / N
  - Are the requirements fulfilled?
    - Y / N
- Recommendations:

  ____

  ____

  ____

  ____

  ____

Managed Services

- Does the Organisation use any Managed Services?
    - Y / N
  - Are they included in the Scope?
    - Y / N
  - If yes; Suitable certifications such as ISO 27001 should be given as evidence.
- Recommendations:

  ____

  ____

  ____

  ____

  ____

Continued on next page

Web Applications and API

- Does the Organisation have a Web App or API?
    - Y / N
  - Is the Web App / API **IN SCOPE**?
    - Y / N
  - If yes, does it have a Web Application Firewall?
    - Y / N
- Give details of the App or API:
- What PII does the Web App or API collect?
- Where is the PII Stored?
- Recommendations:

Continued on next page

Firewalls

- Is the Network Protected by a Firewall?
        - Y / N
    - If No: Install a suitable Firewall
    - Firewall Installed
        - Y / N
- Has the default password been changed in accordance with the Password Policy?
        - Y / N
    - If No: Change Default Passwords
    - Complete?
        - Y / N
- Does the organisation require Remote Administration of the Firewall? (Must be supported by a clear and documented business need)
        - Y / N
    - If No: Turn off Remote Administration in the Firewall Configuration Settings
        - Y / N
    - If Yes: Access to the Administrative Interface must be protected by either
        - A Second Authentication Factor such as a One Time Token
        - An IP Allow list configured to allow access to only trusted and required addresses
    - Protected?
        - Y / N
- Does the Firewall block 'Unauthenticated inbound connections' by default?
        - Y / N
    - If No: Configure the Firewall to block those connections
    - Inbound Connection Rules must be authorised by a competent individual and included in the documentation if required.
    - Required?
        - Y / N
    - Documented?
        - Y / N
- Is procedure in place to remove allowed connections from Firewall Rules when no longer required?
        - Y / N
    - If No: Document the new procedure and inform users who require this information.
    - Complete?
        - Y / N
- Host Based Firewalls should be activated for all machines where access over a non-trusted network (such as a WIFI Hotspot) are required.
    - Activated?
        - Y / N
- Recommendations:

____

____

____

____

____

Secure Configuration

- Has the organisation removed and disabled unnecessary user accounts (such as guest accounts and administrative accounts that won't be used)?
    - Y / N
- Has the organisation changed any default or guessable account passwords to something non-obvious?
    - Y / N
- Have the organisation removed or disabled unnecessary software (including applications, system utilities and network services)?
    - Y / N
- Has the organisation disabled any auto-run feature which allows file execution without user authorisation (such as when they are downloaded from the Internet)?
    - Y / N
- Is the organisation Authenticating users before allowing Internet-based access to commercially or personally sensitive data, or data which is critical to the running of the organisation?
    - Y / N
  - If No for any of above: Carry out required actions
- Recommendations:

____
____
____
____
____

Continued on next page

User Access

- Is a user account creation and approval process being utilised?
    - Y / N
  - If No: Implement 'User Account Creation and Approval Process'
    - Y / N
- Are users authenticated before granting access to applications or devices, using unique credentials (Password Policy Requirements)?
    - Y / N
- Does the organisation remove or disable user accounts when no longer required (when a user leaves the organisation or after a defined period of account inactivity, for example)?
    - Y / N
- Has Two-Factor Authentication been implemented, where available?
    - Y / N
- Are Administrative accounts being used to perform administrative activities only (no emailing, web browsing or other standard user activities that may expose administrative privileges to avoidable risks)?
    - Y / N
- When no longer required, are special access privileges removed or disabled (when a member of staff changes role, for example)?
    - Y / N
  - If No for any of above: Carry out required actions
- Recommendations:

____

____

____

____

____

Continued on next page

Malware Protection
Anti-Malware Software

- The software (and all associated malware signature files) must be kept up to date, with signature files updated at least daily. This may be achieved through automated updates, or with a centrally managed deployment.
    - ▪ Y / N
- The software must be configured to scan files automatically upon access. This includes when files are downloaded and opened, and when they are accessed from a network folder.
    - ▪ Y / N
- The software must scan web pages automatically when they are accessed through a web browser (whether by other software or by the browser itself).
    - ▪ Y / N
- The software must prevent connections to malicious websites on the Internet (by means of deny listing, for example) — unless there is a clear, documented business need and the Applicant understands and accepts the associated risk.
    - ▪ Y / N
- If No: Document the business need
    - ▪ Y / N

Application Allow Listing

- Only approved applications, restricted by code signing, are allowed to execute on devices. The Applicant must:
    - ○ Actively approve such applications before deploying them to devices
        - ▪ Y / N
    - ○ Maintain a current list of approved applications
        - ▪ Y / N
    - ○ Users must not be able to install any application that is unsigned or has an * invalid signature.
        - ▪ Y / N

Application Sandboxing

- All code of unknown origin must be run within a ‘sandbox’ that prevents access to other resources unless permission is explicitly granted by the user. This includes:
    - ○ Other sandboxed applications
    - ○ Data stores, such as those holding documents and photos
    - ○ Sensitive peripherals, such as the camera, microphone and GPS
    - ○ Local Network access
- Is Sandboxing utilised within the Organisation?
    - ▪ Y / N
- Recommendations:

____

____

____

____

____

Software Update Management

The Applicant must keep all its software up-to-date. Software must be:

- Licensed and supported
    - ▪ Y / N
- Removed from devices when no longer supported
    - ▪ Y / N
- Have automatic updates enabled where possible
    - ▪ Y / N
- Updated, including applying any manual configuration changes required to make the update effective, within 14 days* of an update being released, where:
    - ○ The update fixes a vulnerability with a severity the product vendor describes as ‘critical’ or ‘high risk’
        - ▪ Y / N
    - ○ There are no details of the vulnerability severity level the update fixes provided by the vendor
        - ▪ Y / N
- Recommendations:

  ____

  ____

  ____

  ____

  ____