Priya E. Abraham

Your Cyberpower

How to Safeguard Your Remote Business

The author makes no representation or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaims all warranties, including without limitation warranties of fitness for a particular purpose.

The fact that an organisation or website is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organisation or the website may provide or recommendations it may make. Further, readers should be aware that internet websites listed in this work may have changed or disappeared between this work was written and when it is read.

This ebook makes references to the General Data Protection Regulation (GDPR), the ePrivacy Directive and The Directive on Security of Network and Information Systems (the NIS Directive). Clearly, this is not an exhaustive list, but provides the reader with some of the important guidelines for compliance. Readers must inform themselves about applicable national regulations in order to safeguard their business.

Why This Book is for You

Today solopreneurs, makers and start-up entrepreneurs face major challenges when seeking to safeguard their remote businesses.

We live in a world of digital privacy asymmetry. Consumers know very little about the companies and data brokers that know so much about them. Clearly, that is their business. Nevertheless, privacy is personal. It concerns every step we take. It is the data that is harvested about us, bought, sold, and turned into profit.

At the same time policy makers are trying to catch up on regulations to help consumers protect their digital rights. Despite the good intention the regulatory gaps keep getting wider as technology advances ever more rapidly, touching literally every domain of our lives.

As an entrepreneur you must think critically about your displayed digital behaviour, the connected guidelines and cultural principles you use with your networked team, tightly built on cybersecurity including business continuity and privacy including data protection. Routinely, you need to make informed decisions about how to present yourself and your brand in cyberspace whilst protecting your and your clients' privacy.

Your Cyberpower. How to Safeguard Your Remote Business helps you make the essential first step towards establishing digital trust with your users and clients − a branding with which your business should be recognised worldwide.

The book gives you the basic principles behind safeguarding your remote business as well as how to plan your own strategy with key actions to get started. Note: Throughout this book, the terms "users," "customers," and "clients" are used interchangeably to reflect the diversity of your audience.

I wrote this book for non-coding and coding makers, remote workers, solopreneurs including coaches, and start-up entrepreneurs who are responsible for protecting their businesses from cybercriminals and who are liable for guarding the privacy rights of their user base. Your Cyberpower provides an easily digestible introduction to the concept of safeguarding a remote business for business executives who work with solopreneurs and remote workers on a freelance basis.

Icons Used in This Book

This book uses the following icons to indicate special content:

Discover

The Discover icon points out the take-aways of each section that save you time and effort in putting together your own strategy to safeguard your remote business.

Remember

You don’t want to forget this information. It’s essential to gain a basic understanding of safeguarding your remote business.

Implement

Implementation is the key to success. The icon directs you to the Worksheet designed to help you implement the take-aways from the section. The Worksheets are available in the Complete Bundle.

Beyond the Book: Website and Worksheets

Developing, implementing, and enforcing safeguarding your remote business only begins with this book. To learn more, visit *www.cyberconnecting.net*. You’ll find resources including helpful links, free articles, videos, and information on the online course that help explain and manage your route to safeguarding your remote business.

About the Author

Priya E. Abraham is the founder of Cyberconnecting. She is an author, coach, digital transformation strategist and privacy advisor. Priya brings 20+ years of experience in global business across industries, working with established enterprises and with start-ups. In addition to holding a PhD in Business Anthropology and an MBA, she is an accredited Data Protection Officer. Priya has lived and worked in Europe, Russia, the U.S. and MENA. Her experience in all things remote is brought to life in her products and services.

Contents

Chapter 1

Commandeering Your Cyberpower

This section delivers key insights into your cyberpower. It is designed for you to understand its key components and to adapt your behaviours accordingly.

The take-aways of this section are:

- Keep your and your clients' data safe
- Build trust with your clients and users based on your cybersavviness
- Develop a brand awareness built on digital trust

Solopreneurs, makers and start-ups enjoy an unprecedented amount of freedom. For a great number of you, the world is your workplace. Yet with this freedom comes greater responsibility for the cybersecurity of your business and privacy of your customers.

With data breaches affecting more than 1 billion people in 2018, the technology-only promise of cybersecurity solution providers has clearly failed. As human beings, we are the weakest link in this chain. The question is now if technology can ever overcome this shortcoming. As a human being running your own business, it is your responsibility to claim your cyberstrength by combining the best practices from both cyberbehaviour and technology.

This ebook answers the most pressing questions on privacy and cybersecurity while at the same time embracing tech and human behaviour equally to allow you to safeguard your business to build digital trust with your customers. Although we cannot address each and every angle of the challenge, we can easily and simply address some specific examples of best practice.

Let’s first consider a few future forecasts about the freelance community:

- Remote work will become the standard operating mode for at least 50% of the U.S. population by 2020
- There will be 1 billion digital nomads by 2030
- Nomads, remote workers, and makers are all working in the cloud with multiple devices and gadgets (i.e. laptop, tablet, mobile)

As we look at the numbers, two things become clear: firstly, that the common employee is becoming an endangered species; and secondly, that despite the growing competition in the freelance market, you are a major step ahead.

This ebook assumes that you have identified both your key resources and a sellable and scalable digital skill in the cloud and that you are ready to put in the effort to make your business a success.

As mentioned in the introduction, the goals of this ebook are to:

- Encourage you on your path to becoming a great solopreneur, maker or start-up entrepreneur
- Keep you and your business safe so that you can focus on what you do best
- Help you build digital trust with your clients and users to establish a distinguished brand.

Cyberthreats and Data Breaches: The New Normal

As we've mentioned previously, human beings are the weakest link in cybersecurity. Being aware of this fact, you'll need to do everything you can to demonstrate digital competence to your clients and users.

But first, let's understand what data is and why we need to protect our customers' data:

In 2018 the biggest change to the regulatory landscape of data privacy comes with the extended jurisdiction of the General Data Protection Regulation (GDPR). Especially since it applies to all businesses including solopreneurs, start-ups, and SMEs processing the personal data of individuals (also known as data subjects) residing in the European Union (EU), regardless of whether the company's location is in the EU or not. For this reason, it is essential that you as an entrepreneur must understand the concept of personal data.

> ***"Data means any information relating to an identified or identifiable individual; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number (e.g. social security number) or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity (e.g. name and first name, date of birth, biometrics data, fingerprints DNA, ...)."***
>
> ***Definition by CNIL (French Data Protection Authority)***

Remember the number of compromised data sets in 2018?

To put the importance of personal data into context, let us now review how data breaches manifested themselves in 2018:

Organisation	Breaches and Number of Customers Affected*
The Marriott Hotel (Starwood properties group, which includes the St Regis, Westin, Sheraton, Aloft, Le Meridien, Four Points and W Hotel brands)	Half a billion customers
Twitter	330 million users
My Fitness Pal, a food and nutrition app owned by Under Armour	150 million users
Firebase, a Google-owned development platform used by mobile developers	100 million users
Quora	100 million users' names and IP addresses hacked
My Heritage (an online genealogy platform)	92 million user emails and passwords leaked
Facebook	147 million users (in 3 separate breaches)

**** Source: VPN provider NordVPN***

Recent legislation will also likely lead to the reporting of more breaches to law enforcement, as well as increased incidents of cyber-extortion.

So, what does the future hold for cyberthreats?

According to Europol, social engineering remains the engine of many cybercrimes among other key threats, such as ransomware, Distributed-Denial-of-Service (DDoS), and cryptojacking.

“The significance of social engineering for cyber-dependent and cyber-enabled crime continues to grow. Phishing via email remains the most frequent form of social engineering, with vishing (via telephone) and smishing (via SMS) less common. Criminals use social engineering to achieve a range of goals: to obtain personal data, hijack accounts, steal identities, initiate illegitimate payments, or convince the victim to proceed with any other activity against their self-interest, such as transferring money or sharing personal data.”

– IOCTA 2018:8

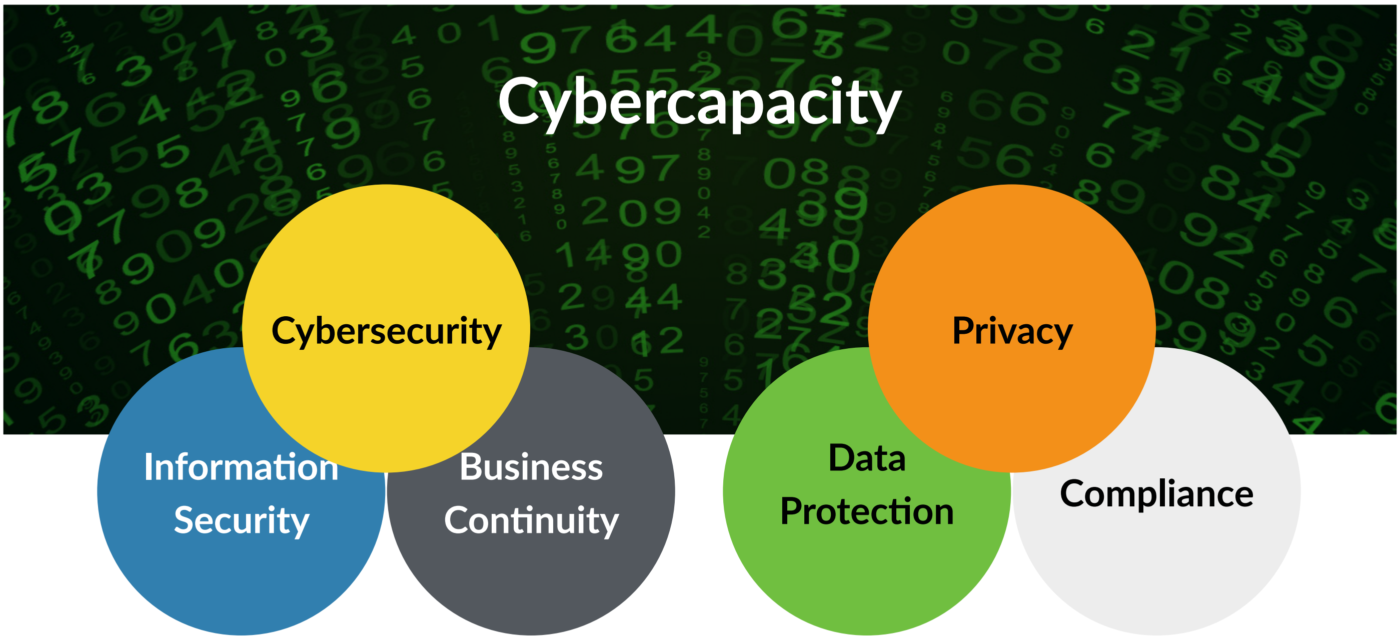
Shaping Your Cybercapacity

Obviously, you're not a big organisation, so you don't have the challenge of setting free the cybersavviness mindset of an entire organisation. But as a brand of one, you are responsible for every single interaction between you, your freelance network, and your clients. As a result, you need to be extra cautious about your cyberbehaviour and act as a role model within your network.

Despite the growing threat landscape, the good news is that as a solopreneur you have the privilege of shaping your individual on-the-road workplace culture conducive to cybersecurity and privacy – in short, you can establish your nomad or solopreneur cyberpower right now.

> “Often data breaches and security related incidents are caused accidentally due to lack of training and awareness, general misconceptions related to data protection and privacy and a lack of understanding of the potential implications of cyberthreats for an organisation. Cybercrime is not a matter of technology alone; it remains human activity. Therefore, it is of great importance to consider the role of human aspects into ensuring *cyber-hygiene*.”
>
> **– Maria Bada, Cambridge Cybercrime Centre**

What are the capacity-building components and why are they important to your business?



It is vitally important that you and your freelance team or network understand the components of cybercapacity. Only when you bring your cybercapacity to life in your daily routines and in your displayed behaviours, then you have developed true cyberpower.

Firstly, cybersecurity isn't the same as data protection, which is more concerned with privacy and how data is used, rather than simply how secure it is. Although it's easy to conflate privacy and security, they're very different things. Think of it like this: putting iron bars across a window adds security but does nothing for privacy; whereas putting a curtain up has the reverse effect.

Cybersecurity is also not the same as data backup, which falls under the domain of business continuity. Having a good backup and recovery scheme in place is vital following any scenario that results in data loss or compromise – whether that's a hack or a fire – but it won't stop an incident from taking place. Nor will it help with mitigation and resolution efforts if an attack is successful.

So, then, what is cybersecurity? The simplest definition comes by way of comparing and contrasting cybersecurity with information security: in simple terms, information security is the protection of your data from any unauthorised access; cybersecurity is protecting it from unauthorised online access. Here is a more formal and comprehensive definition:

> **"Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets."**
>
> **-International Telecommunications Union (ITU)**

Only when you have figured out what cybersecurity means can you begin to plan a strategy and fit it in with business continuity and compliance measures.

What are some behaviours that you can start to put into practice to improve your cyberpower while at the same time strengthening your brand and digital identity?

Three Starter Lessons for Safeguarding Your Business

The number of 2018 data breaches is alarming. Having read this section, you now understand the importance of the key components of your cyberpower. In brief, the key take-aways are:

1. Use the strongest cybersecurity measures you can afford and that you can manage
2. Think twice before posting anything on social media because this information can be used for social engineering
3. Provide online service providers only with the minimum information. The less information you share, the less they can leak

You will find detailed action points and helpful links to each point further on in the document.

“The cyber-threat landscape is evolving daily and under-prepared businesses are the prime targets for financially motivated cyber adversaries. Don’t fall victim to the misperception that only large enterprises are the targets of cyber-attacks. Securing business data is not just a best practice, it’s a business survival necessity.”

– Jarad Carleton, Industry Principal, Cybersecurity Practice at Frost & Sullivan

Chapter 2

Assembling Your Security Toolbox

This section delivers the essentials you need to implement to build trust with your clients with regard to cybersecurity.

The take-aways of this section are:

- Learn how to protect your business against potential threats
- Get to know easy-to-implement cybersecurity solutions
- Understand how to keep your data from prying eyes that want to monetise your data

Let's delve into the three starter lessons above in greater detail.

Use a VPN

A VPN is a uniquely powerful tool that you must have in your security toolbox. VPNs are essential for remote workers and digital nomads, as many of us regularly use airport, hostel/hotel or co-working WiFis. Using public WiFi should be avoided at all costs. But as any solopreneur on the road knows all too well - that is not always possible.

We'll speak about this more at the end of this action point, but for now let's focus on VPN.

So, what is a VPN?

A VPN (Virtual Private Network) allows you to surf the web anonymously and securely from anywhere. VPNs protect you by creating an encrypted tunnel that connects your computer to the internet, WiFi hotspots and other networks. You can install a VPN on your router (highly recommended for smart home devices), laptop, tablet, and smartphone.

A VPN swaps out your internet protocol (IP) address (which identifies your device) for another one. This means that when you switch on your VPN to access the internet, the provider will give you one of their IP addresses, so your IP address remains hidden. In addition, the service encrypts your connection, with the benefit that nothing can be intercepted, seen or tracked.

Why should you use a VPN? It prevents you from:

- Disclosing your web identity
- Being detected by cybercriminals and would-be eavesdroppers
- Exposing yourself to prying eyes that want to monetise your data

When selecting a VPN provider, make sure that their product doesn't leak. Leaks completely undermine the purpose of a VPN, exposing your true location and activities to the prying eyes of your Internet Service Provider (ISP), government agencies, and cybercriminals.

For this reason, we have selected the following, as of 2018 non-leaking, services for your consideration:

	ExpressVPN *www.expressvpn.com/*	**HideMyAss** *www.hidemyass.com/*	**NordVPN** *www.nordvpn.com/*	**Pia** *www.privateinternetaccess.com/*	**Torguard** *www.torguard.net/*
Leaks	No	No	No	No	No
Best for	Security novices	Security novices	General users	Power users	Power users
500+ geographically dispersed servers	Yes	Yes	Yes	Yes	Yes
Jurisdiction	British Virgin Islands	UK, 5 eyes***	Panama	USA	USA
Torrenting *	Yes	Yes	Yes	Yes	Yes
Logging**	No	Store time stamp and IP address	No	No	No

Torrenting connects you to peer-to-peer (P2P) file sharing to download massive files at lightning speeds. ** VPN keeps no records of what you do online. * An alliance of state surveillance agencies known as the 5 eyes includes the USA, the UK, Canada, New Zealand, and Australia.*

Setting up your own network security is easy. However, people are often put off because it seems complicated and often costs money. Free trials are a great way to see which VPN works best for you. But paying for a VPN is a fantastic way to help keep your data secure when you go online.

Using a VPN is completely fine in most countries around the world. See details below in 'Researching Destinations Regarding Safety' in Chapter 3.

Use Strong Passwords

Why should you use strong passwords? Using strong passwords prevents you from:

- Getting locked out of your accounts (e.g. email accounts, online games, bank accounts, credit card accounts, online forums, social networking sites, and every other password-protected corner of the Internet)
- Becoming a victim of identity theft
- Needing time-consuming and costly recovery

Strong passwords, or ones that cannot be easily guessed, meet the following criteria:

- Are at least eight characters long
- Are unique to each login
- Are changed at least once a month
- Contain a mix of upper- and lowercase letters, numbers, and symbols, such as * ?!% _+ and others
- Are changed periodically. A schedule and/or an alarm can be used for this purpose

For convenience you can use a password generator such as *www.strongpasswordgenerator.com*.

Tip: Employ a Lifesaver: A Password Manager

Did you know that the average non-business user has more than 25 accounts? How many do you have as an entrepreneur?

A password manager eliminates the need to remember a long list of unique passwords. You can keep all of your passwords in a special, encrypted programme called a password manager. That way you only need to remember the password manager's master password – a single, ideally very strong password, which grants you access to your entire password database. Password managers usually store encrypted passwords.

A few password managers we recommend that rank highest in PC Mag for reliability and security are:

	1Password *1password.com*	**Dashlane** *dashlane.com*	**StickyPassword** *stickypassword.com*	**Keepass** *keepass.info*
Password generator	Yes	Yes	Yes	Yes
Password changer	Yes	Yes	Yes	Yes
GDPR compliance	1Password.eu are GDPR compliant	Provide for personal rights under the GDPR	Yes, Based in the EU	Yes, installed on machine
2-Factor authentication	Yes	Yes	Yes	Unnecessary because installed on machine

StickyPassword is specifically suitable for you if your business is registered in the European Union (EU), as the provider is based in the EU and follows the necessary compliance applicable in the EU (i.e. the General Data Protection Regulation (GDPR)). Specifically, using this service spares you from transferring your precious data outside the EU. It is also great if your business serves users/clients that are situated in the EU.

Keepass is also registered in the EU. It is open-source (free) and also works in Linux.

Offer Multi-Factor Authentication

When inviting your users to sign up to one of your services, ensure that you offer two-factor authentication (2FA) or multi-factor authentication (MFA). For example, when customers sign up to your email list, 2FA provides you with a way of 'double checking' that the new subscriber is really the person he or she is claiming to be when they are using your online services.

As a user you should also make use of the extra layer of security for your accounts.

Two-Factor Authentication (2FA)

Two-factor authentication is an extra layer of security for your accounts designed to ensure that you're the only person who can access your account, even if someone knows your password. 2FA provides a way of proving a login is legitimate that's completely separate from the password. It is available for Apple ID, Google, Facebook, and Twitter accounts, and other services. For compliance we strongly recommend using services that provide 2FA.

How to Set Up 2FA

Some online services will already have 2FA switched on. However, most don't, so you will need to switch it on yourself to give extra protection to your other online accounts, such as email, social media and cloud storage. If available, the option to switch on 2FA is usually found in the security settings of your account (where it may also be called 'two-step verification').

Set Up a Personal Hotspot (Tethering)

Setting up a personal hotspot, also known as tethering, provides you with an extra layer of security. The personal hotspot feature on your smartphone uses the phone's cellular internet connection to provide wireless connectivity to your laptop, tablet or other devices.

If you have a local SIM card you will not incur roaming as your monthly plan includes the necessary data volume.

- The data used by the devices tethered to your smartphone counts against the phone's monthly data usage limit. Be sure to check the data limit in order to avoid unnecessary costs.
- Keep in mind that tethered connections are usually slower than WiFi connections.

Consider Private Browsing and Messaging

Remember that social engineering remains one of the key threats in cybercrime. This includes phishing, spear phishing (email-targeted phishing from a trusted source), vishing (voice phishing), pretexting (impersonation), whaling (phishing targeting the C-Suite), smishing (SMS phishing) and more. The more you disclose, the more likely you are to become a target. Stay safe by taking back your privacy. Browsing privately keeps your search history undisclosed and helps you escape advertising trackers.

Some Private Browsing Services include:

DuckDuckGo https://duckduckgo.com/app
DuckDuckGo is an internet search engine that protects your privacy. It distinguishes itself from other search engines by not profiling you and by showing all users the same search results for a given search term. It works on every one of your devices; it is easy to install, and it offers a free plan.

Phantom https://phantom.me

The Phantom app is designed for Android users. It keeps you hidden and safe from any kind of tracking, does not share data or sync with other apps of any kind, and keeps your activities invisible - anywhere, at any time. (If you happen to run an NGO, then there is free plan waiting for you).

Remember to provide the same level of privacy to your users and customers that you wish to experience from your service providers.

So, if you wish to keep your clients' data safe, use Fathom Analytics. Their service provides simple, useful website stats without tracking or storing personal data of your users.

Fathom Analytics: *https://usefathom.com/*

Having read this section you now have a selection of best-in-place solutions, from which you can select the one that

- **best suits your needs**
- **is easy to implement and**
- **is cost-effective**

To activate these important cybersecurity solutions, go to the Cyberpower

Worksheet 1: My Cybersecurity Toolbox

Chapter 3

Keeping an Eye on Safety When on the Road

This section provides you with important guidelines to ensure greatest possible safety whilst on the road without curtailing your freedom.

The take-aways of this section help you prevent:

- Experiencing unpleasant surprises
- Compromising your and your clients' data
- Getting into legal trouble

Researching Destinations Regarding Safety

Irrespective of whether you are a digital nomad living in different places across the globe for a few months or a freelancer mainly conducting business in your greater vicinity, you probably conduct some research on the places where you are travelling. As you are carrying your business (i.e. your equipment) with you, keeping an eye on safety is of critical importance for your physical safety as well as your business continuity.

That means that investigating the criminal statistics for different locations in the world are vital for you. For example, you may want to find out what neighbourhoods in Lisbon or New York it might be wise to not visit alone or at night before you arrive in those cities.

Precautionary Steps to Take

Pay attention to what message you are sending to the world with the items that you're carrying and the behaviours you display in your daily routines. For example, carrying around high-end headphones on harrowing streets communicates that you have more expensive tech gear with you. The same applies to other equipment, e.g. a stylish laptop case that can easily be swapped for a plain rucksack that doesn't catch attention. Obviously, wearing expensive-looking clothes can make you an easy target, too.

For a more objective view we advise you to research different sources. Here are some selected services:

nomadlist	*worldnomads*	*gov.uk*	*travel.state*
For the listed destinations you can find scores for all essential items for the nomadic life. Among the categories you can find are: Safety, Traffic Safety, and, for female travellers, a category called Female friendly.	The site offers valuable information on laws, scams, visas and vaccinations you should have before you go.	This site offers latest travel advice for 225 countries or territories including safety and security, travel warnings and potential health issues.	This site offers crime and safety reports for you to assess for yourself the risk of travelling to a particular country or region.

https://nomadlist.com
https://www.worldnomads.com/travel-safety
https://www.gov.uk/foreign-travel-advice
https://travel.state.gov/content/travel/en/international-travel.html

In addition to researching your destinations regarding safety you might want to consider the following:

- Find out the privacy policy of any smart hotel or hostel before you agree to data sharing. These hotels can be used by malicious actors to breach your data. Avoid being hacked by opting out of data sharing in hotels.
- Consider using a tablet instead of a laptop when in transit.
- Turn off WiFi, location-tracking and Bluetooth functions on your phone when you aren’t using them.

Remember the importance of using a VPN?

- Investigate whether the use of a VPN is legal in your destination. Only "Government Approved" VPNs are supposed to be used in China, Iran, Oman, Russia, Turkey and the United Arab Emirates.

Storing Your Devices in a Safe Place

Storing your devices in a safe place requires some extra effort: every time you leave the room you need to put your devices in the safest possible place, whether it's the safe in the hotel room, the specially designed locker in the hostel or with people you trust – but make sure you really trust them!

Never leave your bag or computer unattended. If you're working in a cafe or a co-working place, take your equipment with you. Rest assured, you're not being paranoid; you're being practical and saving yourself from a lot of potential trouble, financial loss and embarrassment. Despite the temptation, never ask a stranger to watch your stuff while you go to the bathroom. This provides you with zero protection against theft.

Precautions to Take

Always put your equipment in a non-visible place. This also applies to power plugs, adapters, and any other additional gear that indicates a laptop nearby.

Don't have all your equipment in one place. For example, if you have two computers, it's better to have them stored in two separate places. If one gets stolen, for business continuity you would at least have the other one.

Be aware that as a business owner you are legally required to store your devices, that is, you and your clients' data, in a safe place. Beyond the legal obligation for data storage, here are some more life-saving tips.

Get a GPS Tracking Device

Alternatively — or additionally — get a device that can track the location of your backpack or your computer: you can install it in a car or a computer, or just carry it separately in your backpack. The tracker typically reports the location to the server.

Encrypting Your Disks

Encrypting your disks is probably one of the most important security measures. It means that when someone steals your laptop, they cannot access the information and data on your machine without knowing your access password (as the data is encrypted). You can easily encrypt your data on Mac by using FileVault. On Windows 10, you can do it with Device Encryption.

Selecting the Right Gear

High-end equipment can make you an easy target for potential theft. Choosing an unpretentious bag for your devices might be one solution to the potential threat; you can also buy a bag called a "security bag". Despite the marketing promises, leaving it unattended is negligent.

Here is a selection of cases:

PacSafe
Wire mesh backpack linings or covers are designed to prevent crooks from cutting into your bag. Zipper locks and hidden pockets should prevent easy theft. *https://www.pacsafe.com/*

Pelican
High durability backpacks ensure that laptops and additional equipment are protected by storing them in built-in watertight, crush-proof cases. *https://www.pelicancases.com/products/backpacks-and-bags*

Buying Appropriate Insurance

Today we often fall between the cracks, without access to insurance and a national safety net. So, it is best to look for your own global safety net that meets your needs as a solopreneur or remote worker. The following services typically provide: travel medical, travel, and lost, stolen or damaged belongings.

In addition, some have a community service such as connecting with like-minded travellers. They serve all age groups; they are available for shorter trips and for long-term travel. They typically offer a standard and a premium plan. Check here what suits you best:

Safety Wing
https://www.safetywing.com/

WorldNomads
https://www.worldnomads.com/travel-insurance/

TravelGuard
https://www.travelguard.com/

Having read this section, you now have practical advice to avoid

- putting yourself and your equipment at unnecessary risk
- worrying about a potential accident and
- having to cover the costs of a lost, stolen or damaged device out of your own pocket.

To make use of the practical advice go to the Cyberpower Worksheet 2: Safety on the Road.

Chapter 4

Ensuring Business Continuity

This section provides you with practical advice to ensure your remote business's continuity and prosperity.

The take-aways of this section help you prevent:

- Losing market share
- Jeopardising your brand reputation
- Interrupting your communication with your remote business network

What is business continuity? Business continuity is planning to make sure that you are prepared for any serious incidents or disasters and that you can resume normal operations within a reasonably short period – whether your business was interrupted by fire, theft or cyberattack. A business continuity plan typically covers business processes, assets, human resources, business partners and more.

Taking Preventative Steps in the Event of Theft or Disaster

Here are some valuable tips to give your remote business the best chance of avoiding or surviving such an event.

Firstly, remember the importance of always locking up your devices? Also lock up your power plugs, adapters, and any other additional gear that indicate a laptop nearby.

Remember never to leave your devices unattended, not when getting a coffee in a café or just quickly going to the bathroom.

- Take a backup device wherever you go, even if it’s just an old but functional phone or tablet. Store it in a safe, accessible place so that it is available in case of an incident of theft or disaster. You will need to inform your clients and your network about a short delay and to communicate with the authorities.
- Use ‘Find My Device.’ Apple has its own system of detecting the location of your devices called Find My Device. Windows has a similar option as well as Android devices.
- Create regular backups. Many people neglect this simple measure. As a freelancer, you should know better. Use a cloud service or an external disc to create regular backups. For you - more than anyone else - data is currency, and data loss equals earnings loss.

The greatest weapon against ransomware is an up-to-date backup. If you regularly back up your work, you'll never have to pay the ransom or an expert to de-encrypt your data, because you can always wipe your machine and restore it. In that case an attack will cost you time, but no money.

Start with these steps and consider adding more to your written recovery plan as time goes on. You will find more hands-on advice at the end of this section. Remember, it is vital for establishing your brand that your customers are able to trust you with their data and information.

What to Do in the Event of a Lost or Stolen Device

After recovering from your initial shock, take time to think back to how the loss of your device occurred.

Try to retrace your steps and remember where you may have left it. If you think you may have lost it at a retail store or any other semi-public place, check with the people in charge to see if they found the device lying around. You might be lucky.

However, once you are certain that it can't be recovered you have to contact the authorities. As a victim of a crime, you must report the incident to the authorities. If you want to claim the stolen device for insurance purposes, you will need to present a police report.

For those working at a co-working place or hostel: if you believe a co-worker or fellow hostel resident has stolen your device, immediately contact the manager.

As an entrepreneur you will hold the personal data of your clients and users on your stolen device. As a result, you will need to report the loss to the Data Protection Authority (DPA) of the country in which you are incorporated. See the Data Breach section for details.

Building Your Business Continuity Plan

Now that we have covered some essential preventative steps and some actions to be taken in case of a lost or stolen device, let us look at the bigger picture of business continuity. This includes

- identifying the risks that would most likely disrupt your operations
- identifying critical functions for staying in business, e.g. bringing a back-up device; and
- building a recovery plan that covers the needs of your remote business.

Here's the full picture:

1. know your risks
2. know your operations
3. know your finances
4. know your information technology
5. know your freelance network
6. know your suppliers, vendors, users, and key contacts
7. know when to update and test your plan
8. know where to go for help

Building a plan is one item on our to-do list that easily gets put off indefinitely. We all have to focus on today's challenges, so it is important to devote time and attention to your business continuity plan. We have already mentioned a number of risks and measures you should include in your plan throughout the sections.

Having read this section, you now have practical advice to

- **remain competitive and minimise the loss of revenue and users**
- **show that your remote business is committed and prepared to protect your networked team, customers and assets at all times**
- **improve your daily operations and your communication with your community.**

So, stop making excuses and start making your unique business continuity plan! Go to the Cyberpower Worksheet 3: Ensuring Business Continuity.

> “With remote work you’re asking your clients to trust you with their business. Being proactive about privacy and security proves that you want to take the best care of them. The best - not just ‘only sufficient because we haven’t been audited yet’. Your proactiveness becomes their compliance guarantee.”
>
> –Sebastien Vercammen, Maker

Chapter 5

Ensuring Privacy

Closing the Curtains for Greater Privacy

Remember, putting iron bars across a window adds security, but does nothing for privacy. Putting up a curtain has the reverse effect. With more than 1 billion users affected by the data breaches committed in 2018, you'll need to be sure to both put iron bars across your window and put up a curtain to safeguard your business. Only with combined cybersecurity and privacy efforts can you keep yourself and your clients' data protected.

2018 was a big year for national and global privacy data laws to come into effect - to name a few, the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the Israeli Data Security Regulation.

In early 2018, much focus was placed on the draconian GDPR fines of up to 4% of the annual turnover of the previous year (or a maximum fine of 20 million Euros). The new laws have already demonstrated an effect: In January 2019 alone, Google was fined 50 million Euros by the French data regulator CNIL for a breach of the EU's data protection rules - specifically for "lack of transparency, inadequate information and lack of valid consent regarding ads personalisation".

Stay aware of these laws and use them to build a trusting relationship with your client base. Many automated security and privacy solutions are convenient tools; nevertheless, they are typically designed for larger enterprises. They tend to be too expensive for solopreneurs and bootstrapped start-ups. However, as soon as your business scales, budget for selected automated solutions. For now, keep it simple – select third-party providers who are GDPR-compliant, select low-cost privacy solutions or start building spreadsheet lists where you need to keep a record.

By putting your clients' personal data at the heart of your business processes, you will be moving quickly beyond tick-the-box compliance and build genuine digital trust with your clients.

Commandeering the Essentials

This section delivers selected key points of the GDPR. It is designed for you to get started with your privacy essentials straight away.

The take-aways of this section are:

- Familiarise yourself with the key terms and their implications for your remote business
- Understand your best choice for gaining user consent
- Learn to evaluate the suitability of third-party providers with regard to privacy

Understanding Personal Data

At the heart of the EU General Data Protection Regulation (GDPR) is personal data, which in brief means 'any information relating to an identified or identifiable natural person, also known as data subject'. In other words, any information that is linked or can be reasonably linked to a particular individual (data subject).

Remember that the majority of location-independent businesses collect and use personal data. For this reason, it is essential that you understand the concept of personal data.

If you collect, store, or use any of the following: name, address, localisation, online identifier, health information, income, or cultural information, then you have to abide by the rules applicable for personal data.

- Are you a data processor or a data controller?
- Do you know the difference? Find out here if you are a processor or controller: *https://gdprchecklist.io/*

Arguably, the biggest change to the regulatory landscape of data privacy comes with the extended jurisdiction of the GDPR. In other words, if you are processing the personal data of users, (e.g. their first name, family name, email address), then the GDPR applies to your business activities; even if your business is registered outside the European Union (EU).

In more detail, this means that the Regulation applies to the processing of personal data of data subjects who are in the EU by a controller or processor not established in the Union, where the processing activities are related to:

a. the offering of goods or services, irrespective of whether a payment by the data subject is required, to such data subjects in the Union; or

b. the monitoring of their behaviour as far as their behaviour takes place within the Union.

In addition to the changes to the regulatory landscape the GDPR enhances the rights of data subjects in the EU. Among others, they have the right to request access to and erasure of their information. In addition, you need to provide greater transparency on your personal data processing activities, with clear and easily understandable information on processing. Making this information available gives your data subjects insight into how their information is used. The catalogue of rights is much wider - selected details of individuals' rights will be presented in the next section.

Beware: Requests to exercise data protection rights are a sign that your users have a trust issue with your business.

Guiding Principles of the GDPR

The guiding principles of the GDPR are captured in legal lingo.

Here is a translation into best practices of selected guiding principles:

Best Practice	Legal Term in Official GDPR text
Collect and process as little personal data as necessary	Data minimisation
Establish a reason for processing the personal data	Lawful basis
Make data privacy your default action: build it into all your organisational and technical processes	Privacy by design

Gaining User Consent

You have all seen the tick-boxes that you need to click to give consent in order to subscribe to a newsletter or to use any other service. Do you find this irritating? You shouldn't, as it gives you the possibility to exercise your rights as a customer.

Since you probably don't want to afford the fines Google has incurred in violation of GDPR - even adapted to your circumstances – you must ensure that you obtain the consent of your future subscribers and users properly. Only then are you expressly allowed to process their personal data.

Did you know that consent is only one of the so-called six lawful bases to process personal data in the General Data Protection Regulation?

The others lawful bases are: contract, legal obligations, vital interests of the data subject, public interest and legitimate interest as stated in Article 6(1) GDPR. As a freelancer, the other likely lawful basis is contract, which occurs when the processing of personal data is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

For details of the other four lawful bases see: ico.org.uk

The business model of nomads and freelancers is often based on building a mailing list and on growing it rapidly. For this purpose, a landing page with sign-up options and regular newsletters are still known as the smartest, leanest, and most cost-effective ways to grow the business.

Sending e-mail direct marketing is subject to the ePrivacy Directive and its national implementations. Ensure that you also inform yourself about applicable national regulations in order to safeguard your business.

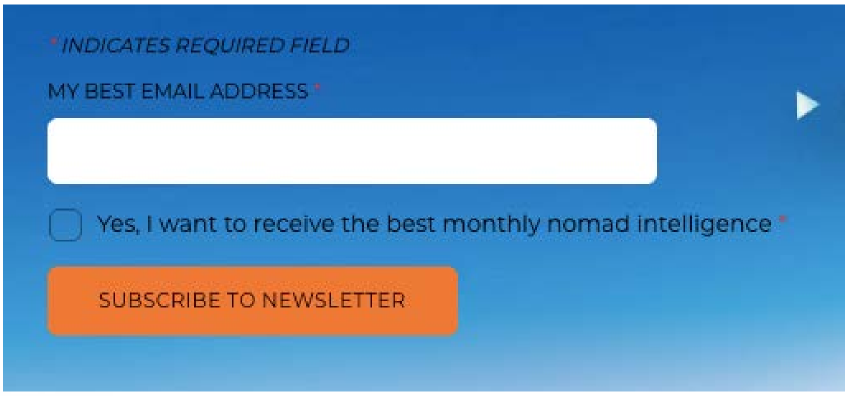
Your newsletter sign-up should:

- Ensure that the subscribers to your newsletter give you their consent freely and specifically
- Use their personal data only for the purpose of the newsletter and not for any other of your services
- Consider the guiding principle of data minimisation (i.e. when designing the fields for the sign-up ask for the bare minimum of personal data)

All e-mails sent must contain an unsubscribe feature that can be used easily and free of charge.

Here are examples of good and bad practice for gaining user consent:

Good practice



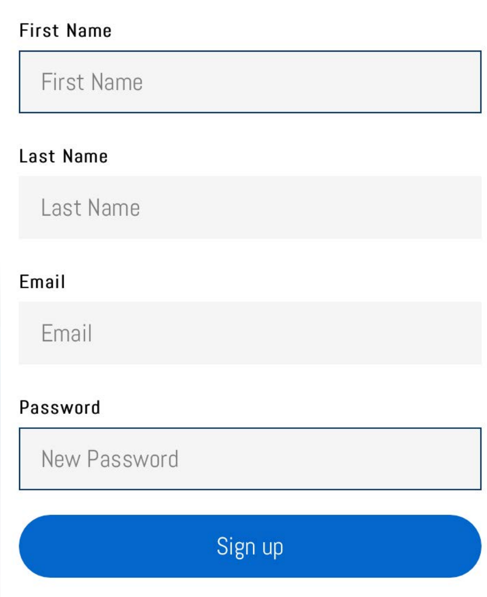
* INDICATES REQUIRED FIELD

MY BEST EMAIL ADDRESS *

□ Yes, I want to receive the best monthly nomad intelligence *

SUBSCRIBE TO NEWSLETTER

Often spotted bad practice



First Name

First Name

Last Name

Last Name

Email

Email

Password

New Password

Sign up

Remember the extra layer of security presented in the security toolbox – the two-factor authentication? Provide your users with the same layer of security. It also gives you the possibility to verify the user's identity.

Beyond your digital offering and the connected necessary consent, you also have to consider consent in case you facilitate events for further promotion of your offering. Circulating a participant list and having the participants sign does not suffice to include their personal data on your mailing list. You specifically need to ask for consent for the newsletter mailing.

It must be as easy to withdraw consent as it is to give it. Consent has strict requirements, including the fact that it can be withdrawn at any time.

In other words: If one of your subscribers unsubscribes from your list, make sure not to send any further newsletters to this person.

The lawful basis for your processing can also affect which rights are available to individuals.

However, remember that an individual always has the right to object to processing for the purposes of direct marketing, whatever lawful basis applies.

You Must Keep all Records:

The GDPR requires you to maintain records of the type of data you hold, where it came from and with whom you share it, all of which requires documentation.

If you use a third-party provider that offers GDPR-compliant consent management, they typically offer a mechanism for record keeping, e.g. MailChimp. Your audience lists typically show how and when people subscribed.

Tips for Best Practice:

Review the record regularly, export it, and have it available in case of an inquiry from a Data Protection Authority.

If you are using a provider that does not offer this service, ensure that you create a record, keeping it updated and available for possible inquiries.

The individual's right to be informed under Article 13 and 14 of the GDPR requires you to provide people with information about your lawful basis for processing. This means you need to include these details in your privacy notice. See details in the next section.

Selecting Third-Party Providers

When selecting a content management system, an email automation provider, an online course provider, etc. consider the following best practices before entering a contract with them:

- Confirm that they are compliant with the privacy laws applicable to your context
- If located in the U.S or Switzerland, ensure that they have participated in and have certified their compliance with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework.
- List the provider in your record of processing activities
- Ensure that you have signed a third-party contract with the provider and that you can make it available to the authorities upon inquiry

Having read this section, you now understand the importance of

- **personal data**
- **gaining consent, and**
- **selecting third-party providers.**

To activate the three key points, go to the Cyberpower Worksheet 4: Privacy. Commandeering the Essentials.

Progressing to the Next Level

To build digital trust with your users and clients you need to inform them how you use their data, which of their behaviours you track (if any) and, in case of a mishap, how you liaise with the authorities.

The take-aways of this section are:

- Learn how to generate your privacy notice
- Set up a cookie policy for your landing page/website
- Identify the authority in charge for your business

Developing Your Privacy Notice

A privacy policy is mandated by law. Nevertheless, looking at it as only a legal nuisance is a lost opportunity. Your privacy notice should help your website/landing page visitors build trust.

What you should tell your users:

- what information you collect. (e.g. first name or both names, email address, credit card, account or PayPal details and any other information relevant to the interaction you have with visitors to your site)
- why you are processing their information (check back with the lawful bases)
- how you collect the data (e.g. newsletter forms, contact forms, comment systems)
- how long you store it for and how you protect it
- whether there are other recipients of their personal information (e.g. third-party providers such as social widget providers, external account access services, payment processing services, email and newsletter management services, tracking and analytics, ad services)
- whether you intend to transfer it to another country (this applies to the services listed above), and
- whether you do automated decision-making or profiling.

Make sure that you keep your privacy notice updated. Upgrading your services typically means that you need to review your privacy policy and rework it accordingly. Attempting to write a policy notice can be a scary thing if you don't have a legal background or haven't worked with the matter professionally. Equally, hiring legal assistance can be quite resource-intensive. So, in the light of the solopreneur or maker spirit, here are some of the best privacy policy generator tools you can use to create a privacy policy template page for your website:

1. *https://www.iubenda.com*
2. *https://www.privacypolicies.com/*
3. *https://www.termsfeed.com/*

Use a privacy policy online tool but do your research and seek legal advice if you need to. Bear in mind that these sites use standard templates; you'll need to add or edit such a template to satisfy all the needs of your business. Seek legal advice and have your privacy policy reviewed by an expert. You should also find out what the legal requirements are for where your business is incorporated (not where you live), as privacy policies are mandated by law in many countries.

Setting Up Your Cookie Policy

A cookie is a small text file that is downloaded onto your user's device (e.g. a computer or smartphone) when the user accesses your website. It allows your website to recognise that user's device and store some information about the user's preferences or past actions. When cookies can identify an individual via their device, it is considered personal data.

Not all cookies are used in a way that could identify users, but the majority are and are therefore subject to the GDPR. This includes cookies for analytics, advertising and functional services, such as survey and chat tools.

What you have to do to be compliant:

- tell people the cookies are there;
- explain what the cookies are doing and why; and
- get the person's consent to store a cookie on their device.

As long as you do this the first time you set cookies, you do not have to repeat it every time the same person visits your website. However, since some devices may be used by different users, you may want to consider repeating this process at suitable intervals.

With regard to consent, make sure there is genuine and free choice. For example, when ticking a box or clicking a link your users must fully understand that they are giving you consent. You must also make it possible to reject cookies. Even after getting valid consent, your site must give people the option to change their mind. If you ask for consent through opt-in boxes in a settings menu, your users must always be able to return to that menu to adjust their preferences.

You can use pop-ups or 'splash pages' to make your users aware of the use of cookies and to obtain their consent. Make sure that you select a well-designed option developed to ensure that you don't spoil the experience of using your website.

For your convenience, we sourced some helpful solutions:

1. *https://www.cookiebot.com*
2. *https://www.iubenda.com*
3. *https://www.civicuk.com*

Understanding the Data Breach Notification Requirement

The GDPR has a strict data breach notification requirement, stating that organisations have only 72 hours to report a breach to supervisory authorities, which is sometimes easier said than done. It has become ever more difficult to track data flows and guarantee that sensitive data is not exposed.

Note: Remember the steps to take in case of a lost or stolen device described earlier? On the assumption that you hold the personal data of your users, you have to report the loss to the Data Protection Authority (DPA) of the country in which you are incorporated.

In the event of a data breach, assess how the breach affects individuals. To do this, you must know what sensitive data you hold, where it resides, who has access to it, and how the data is classified according to its sensitivity. This will help to identify what data was compromised, the impact the breach has on individuals, and whether you must notify the DPA or even the data subjects directly.

For example, if you are an Estonian e-citizen and have incorporated your business in Estonia, you need to report the breach to the Andmekaitse Inspektioon, the Estonian DPA: *www.aki.ee*

Those based in another European country need to report to their local Data Protection Authority (DPA). If your business is registered in Austria, for example, you need to report a breach to the Austrian Datenschutzbehörde: *https://www.dsb.gv.at/*

Find the full list of DPAs here:
https://edpb.europa.eu/about-edpb/board/members_en

For organisations based outside the EU, this responsibility lies with their European Representatives, who are obliged to report to their local DPA as well.

In general, we strongly recommend that you source a legal representative specialising in data protection registered in the country of your incorporation. In the event of an alleged data breach, you need to act fast. Hand the case over to a professional rather than trying to fix it yourself (unless you are a privacy expert). Perhaps the allegation is minor and fixing the issue could require only a letter in legal wording. Make sure that you have a minimum budget available for such an incident. If you are incorporated in Estonia and you need professional advice, contact Mr. Mihkel Miida, Head of Technology & Data Protection at Sorainen

www.sorainen.com
His email address is: ***Mihkel.Miidla@sorainen.com***

Having read this section, you now understand the ways forward to

- developing a privacy notice
- setting up a cookie policy, and
- taking the necessary action in case of a data breach.

To activate the three key points, go to the Cyberpower Worksheet 5: Privacy. Progressing to the Next Level.

Chapter 6

Securing Your Brand with a Data and Privacy Strategy

Although this ebook is not meant to be exhaustive, it should point you in the direction to go for further assistance. That's why it's imperative that you develop strategies for managing personal online information and keeping it secure from online risks such as identity thieves. You'll also want to develop enough cyber self-awareness to become resilient to attacks or data breaches.

Remember that at the end of the day, your nomadic digital identity is dependent on you, your interactions, and your brand. This includes how your data and privacy strategies function with regard to customers as well as your day-to-day behaviour.

As an entrepreneur, you are liable for the cybersecurity of your business. Everyone who works towards the success of your business needs to do their bit to ensure your business is protected against any threats that could put it at risk. But most importantly, as the head of cybersecurity for your business, always remember that you are the role model demonstrating the necessary behaviours on a daily basis. Follow the guidelines in this ebook and you'll start to safeguard your brand while boosting your cyberpower and reclaiming your cyberstrength at the same time.

Learn more in the bonus chapter 'Your Cyberpower Brand Identity', available in the Complete Bundle.

References

https://www.bbc.com/news/technology-46944696

https://www.cnil.fr/en/personal-data-definition

https://www.computerweekly.com/news/252455311/Data-breaches-affected-more-than-a-billion-people-in-2018

https://edpb.europa.eu/about-edpb/board/members_en

https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018 (IOCTA 2018)

https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/take-control-of-your-digital-life-don%E2%80%99t-be-victim-of-cyber-scams

https://www.forbes.com/sites/abdullahimuhammed/2018/12/21/10-remote-work-trends-that-will-dominate-2019/#688434c97c72 *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/*

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/#ib3

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/

https://levels.io/future-of-digital-nomads/

https://www.securityinfowatch.com/article/12431013/vigilance-required-in-an-evolving-enterprise-threat-landscape

https://thebestvpn.com/vpn-leak-test/

https://uk.pcmag.com/vpn/138/the-best-vpn-services-for-2019

The world is my workplace.