POLICY AND COMPLIANCE COLLECTION

SELF-STUDY WORKBOOK

IT Security for the Remote Worker and Business Traveller

More people are working remotely than ever before.

If you're working from home, or travelling for work, no doubt you'll have some level of IT with you.

We doubt you're working off an abacus.

And anywhere you've got work-related IT, you need the same level of security that you'd have if you were sat at your desk. Maybe even more.

Yes, the rules are a little different.

But luckily, this workbook can help.

Peruse away.

NAME _____

LITMOS HEROES

Saving the world from boring learning

HOW TO USE THIS WORKBOOK?

This workbook outlines all the key things you'll need to know to keep your remote working devices and data safe.

It's presented in bite-size chunks in an accessible way – there won't be anything too jargon. Plus, there's takeaway sections dotted throughout to aid your retention.

On top of that, there's a little question section at the end. Using the info shortly after learning it helps transfer it to your long-term memory. Handy that, isn't it?

Who should use this workbook?

- Employees who work remotely or travel for work
- Employers with staff who work remotely or travel for work
- Anyone interested in picking up some useful IT security tips

Key Insights

- Definitions and context
- Breach risks
- Consequences of breaches
- Some solutions
- The importance of backing up

POLICY AND COMPLIANCE COLLECTION
SELF-STUDY WORKBOOK

THE BACKGROUND

37% of US workers say they've worked remotely (Gallup).

There are 4x as many workers telecommuting now than in 1995, thanks to tech advancements and lower costs.

That means a lot of people out of the office. Which means a lot of data out of the office.

And that's a risk.

Did you know?
90% of large businesses
74% of small businesses
▶ have reported some level of information security breach.

The consequences can be severe. Besides any reputational damage and theft of confidential information, there's the financial costs.

Cyber-crime has cost around $388 billion in losses.

To put that in perspective, the market for heroin, marijuana and cocaine stands at $288 billion.

Of course, bigger businesses have huge financial losses, but it's the smaller businesses that are, proportionately, hit harder. The average expenses from a single data breach are around £38,000, before fines (Kaspersky).

We'd be surprised if you already knew:
Around 90% of breaches are caused by human error.

When you're working out of the office, a lot of these problems are made worse by the fact that it's an unfamiliar setting. That means the rules are a little different. Your organisation has less control over the environment.

TAKEAWAY

There's serious risks when it comes to cybersecurity, and they can be exacerbated by remote working.

Make sure you're as vigilant, if not more so, when working away from your desk.

THE RISKS

We expect you already know about IT risks when you're in work, so we'll use this section to look at ones specific to remote working.

They can be split into two categories: physical risks and electronic risks.

Physical risks

These are the most obvious, and involve something physically happening to your data or devices.

For example, you could lose your laptop or phone. You could drop them in the toilet, or the dog could chew them up. Far more likely to happen with a mobile device than a desktop.

There are also visual threats. Someone peeping over your shoulder, or "shoulder surfing", could spy important information like usernames or passwords. They could hang around hotspots like cafés or waiting rooms, and could even take photos or record conversations.

How could you possibly know?
82% of workers admitted there's a chance someone has shoulder-surfed them while working.

Electronic risks

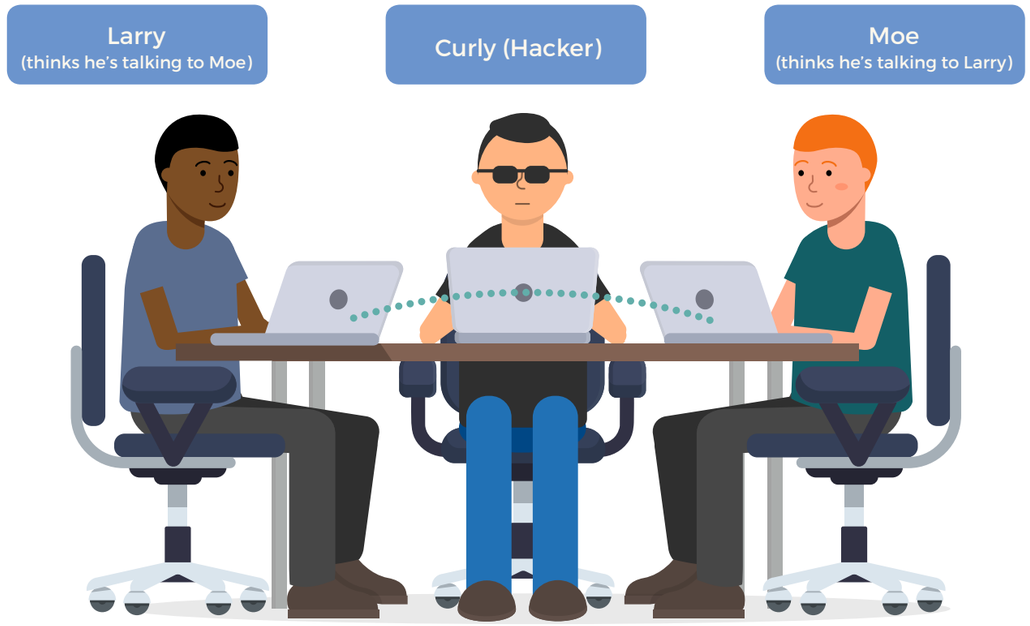
Unlike office equipment which can be looked after by an IT team, remote worker-owned devices mightn't be equipped with adequate security protection. Things like firewalls and anti-malware. That means data can be "phished" – gained fraudulently through disguised data entry points – more easily. There's also the risk of session hacking, where hackers take over sessions when the user logs on.

Insecure Wi-Fi is another danger. Coffee shops, train stations – anywhere with unsecured Wi-Fi – can be a source of a data breach.

Don't pretend you knew:
89% of public Wi-Fi hotspots are unsecured. (FBI)

POLICY AND COMPLIANCE COLLECTION
SELF-STUDY WORKBOOK

Man-in-the-Middle attacks (and no, it doesn't have to be a man) are where hackers bug connections or network cables, making independent connections with multiple victims and relaying messages between the two. Like this:



File sharing is another biggie. The Cloud? It can result in data leakage if the right controls aren't in place. Emails, too. They're also used in the office, but there may be more strict protocols there than when working remotely.
Unauthorised, unsecure apps are also problematic when it comes to keeping data secure.

You definitely never knew:
70% of IT professionals believe unauthorised programs lead to at least half of their companies' data-loss incidents. (Cisco)

USBs and peripheral devices are a further risk, if they've not been checked out for safety. They could contain malware.

TAKEAWAY

You can see there's plenty of risks, and plenty of points of vulnerability.

You can split them into physical and electronic risks, but they're both as serious as each other.

ACTIVITY

What risks can you spot in this scene?

Point them out with your finger. No-one's actually checking, but do do it. It's important to your business.

If that doesn't work, reverse psychology: Bet you can't get them all. What are you, chicken? Buk buk...

POLICY AND COMPLIANCE COLLECTION
SELF-STUDY WORKBOOK

THE SOLUTIONS

Let's look at the solutions in the same way we looked at the risks. We'll start with splitting them up, and tackling the physical first.

Physical solutions

- Sounds like a cop out, but one of the best ways to avoid physical hazards is simply to stay vigilant. There's no software that'll stop you dropping your cellphone down the toilet (yet).
- Keep your screen away from prying eyes, or covered. Watch out for reflections, etc. Kind of like how you'd act at an ATM. And keep your eyes on your devices at all times.
- Test yourself on things like always storing devices out of sight when you leave home, locking your screen when it's not in use, having separate accounts with distinct password for work and personal use, and ensuring any shared family use doesn't accidentally allow access to the work domain.
- Don't let friends or family use your work devices, period.
- In terms of breakage, you could consider ruggedised equipment, cases and other protective accessories, or maybe just not being such a klutz.
- You might also want to try 'Find My Phone' type applications in the case of lost devices.

Electronic solutions

- Golden rule – never use public Wi-Fi for sensitive info. Only connect to trusted networks and never use 'save password' or 'remember me' functions. Use private browsing if available.
- Keep an eye out if you suspect phishing or any other scams. Treat everything with a healthy scepticism.
- Encrypt files when you remove information from the workplace.
- Equip your devices with up-to-date virus protection software.
- Back up your information regularly. The next section has more info on this.
- Have your IT team look at your security policy, as well as having them check out 3rd party applications and software. Get a list of approved apps if necessary. accessories, or maybe just not being such a klutz.
- You might also want to try 'Find My Phone' type applications in the case of lost devices.

TAKEAWAY

With both physical and electronic solutions, as with everything, a lot of it is just a case of really thinking things through.

Treat all your work equipment with the utmost care, and you should do okay.

THE BACK-UP

A data backup involves making copies of critical and sensitive computer data on alternative storage devices. If your laptop or mobile device is stolen or corrupted by malware or a virus, your data can be restored.

It's so easy to lose data, and impossible to automatically rebuild your data if backups don't exist. That's why they're so important.

Doubt you knew these:

- A third of IT Admins don't test backup solutions for effectiveness.
- A third of employees don't do a daily backup because they think it's not an efficient use of their time.
- And, in almost half of cases, it takes less than an hour to back up business-critical files and applications. (GFI)

As a remote worker, if you don't have access to your company's backup system then you are responsible for backing up your devices. There are serious consequences if you don't: permanent loss of business-critical data, business, legal and regulatory penalties, losing out to competition, or the inability to resume business.

You might actually have known this:

The whole Pixar movie Toy Story 2 was accidentally deleted during production, after months and hundreds of hours of effort. The backups they had were corrupt, and the project was in serious trouble. Luckily, one employee saved the day – she had backed up the files directly to her PC.

Here are some tips for backing up your data:

- Make a clear plan and identify all critical and sensitive data to be backed up.
- Use tested software and schedule your backups.
- A popular method used is three-two-one. This means three copies of your backup, with two on alternative media and at least one in a different location.
- Identify a reliable source device for backup with durable recovery capabilities.
- Avoid backing up on thumb drives (these tend to get misplaced, lost, or fall into unwanted hands).
- Secure your backup by protecting your backup data with a password or encryption.
- Test your backup at least once every 6 months by recovering your backup and making sure it really works.

POLICY AND COMPLIANCE COLLECTION
SELF-STUDY WORKBOOK

THE PASSWORDS

You need to have proper password controls in place. This applies both in the office and when you're out and about.

Put 'guest', 'password', '123456' and 'qwerty' in the bin.

In fact, your password shouldn't even be a word in the dictionary, or a proper noun like your children or pets' names.

A good, secure password meets the following criteria:

- Eight or more characters
- Upper and lower case letters
- Numbers
- Symbols

All those numbers and symbols can be tricky to remember, so try using a mnemonic device.

Two-factor authentication is also a useful tool. That means having both a password and a linked email or contact information to confirm it's really you accessing your work material.

TAKEAWAY

Backing up and having appropriate password controls are two really important methods of keeping your data safe.

Learn how best to carry them out, and don't underestimate.

QUIZ

We promised you questions and by Jove, Mars and Juno, you'll get them.

Answer these and it'll help the learning stick, and so ultimately help you stay safer when working remotely.

1 **What are some of the key physical risks, and some solutions?**

---

2 **What are some of the key electronic risks, and some solutions?**
(saw that coming, didn't you?)

---

3 **What are the criteria a good password has?**

---

4 **Why is backing up so important?**

POLICY AND COMPLIANCE COLLECTION
SELF-STUDY WORKBOOK

FINAL SUMMARY

Well done! You've passed the IT Security for the Remote Worker and Business Traveller course!

Now, you know the importance of IT security, and the potential consequences of lapses.

You also know what sort of IT security hazards to look out for, both physical and digital, and a few of the ways you can protect yourself and your company.

You know about the importance of backing up and best practice, as well as how to craft a solid password.

Plus, all this:

- Best practices for working remotely or telecommuting.
- How to safely work on your laptops and mobiles in public places, and connect to public hotspots.
- How to be aware of shoulder surfers.
- The importance of IT security, and the potential consequences of lapses.
- What sort of IT security hazards to look out for, both physical and digital, and a few of the ways you can protect yourself and your company.

But these tips aren't, and can't be, a catch-all.

Technology's constantly evolving. That means the risks are always changing.

The better informed you are, the easier it'll be for you to stay safe.

If your organisation has an IT department, make sure to stay on top of any updates to software and policy that it makes available.

That way, you can feel secure going back to the glamorous world of working away from the office.

LITMOS HEROES
Saving the world from boring learning