CYBER SECURITY COLLECTION

SELF-STUDY WORKBOOK

Cloud Computing

The Cloud is absolutely everywhere these days. And we're not on about the weather.

There's a good chance you're using it where you work, or if you're not now, you could be soon.

Thing is, like virtually everything else, you need to stay safe while using it.

If you don't, you could end up losing a lot more than just some data.

This workbook is going to show you how to keep on top of it all.

NAME ______________________________

LITMOS HEROES

Saving the world from boring learning

www.LitmosHeroes.com

HOW TO USE THIS WORKBOOK

It's not like this workbook can actually keep an eye on your data, computers or behaviour.

The way it works is you go through it, learn the stuff, and then put it into practice.

It'll also mean you liaising with your IT team to work on any issues specific to your business.

We'll present the key info for you in logical sections, with a takeaway at the end of each with the key learning for you to remember.

There's also a Q&A at the end to help the learning stick in your memory banks.

WHO IS THIS FOR?

- Employers who'd like their staff to be knowledgeable about Cloud systems
- Staff who'd like to know how to keep company data secure
- Anyone who works with computers using the Cloud (which is probably most of you)

KEY INSIGHTS

- What the Cloud is and what its uses are
- The main methods of Cloud deployment
- Cloud services and common examples of them
- The crucial role of cybersecurity in all types of Cloud computing

CLOUDY DAYS

Before we start talking about the Cloud, we need to know what it is.

According to the National Institute of Standards and Technology, it's:

Convenient, on-demand network access to a shared pool of configurable resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Putting that in a less technical way, it's a data storage and usage network that allows greater data self-governing and scalability than previous computing methods.

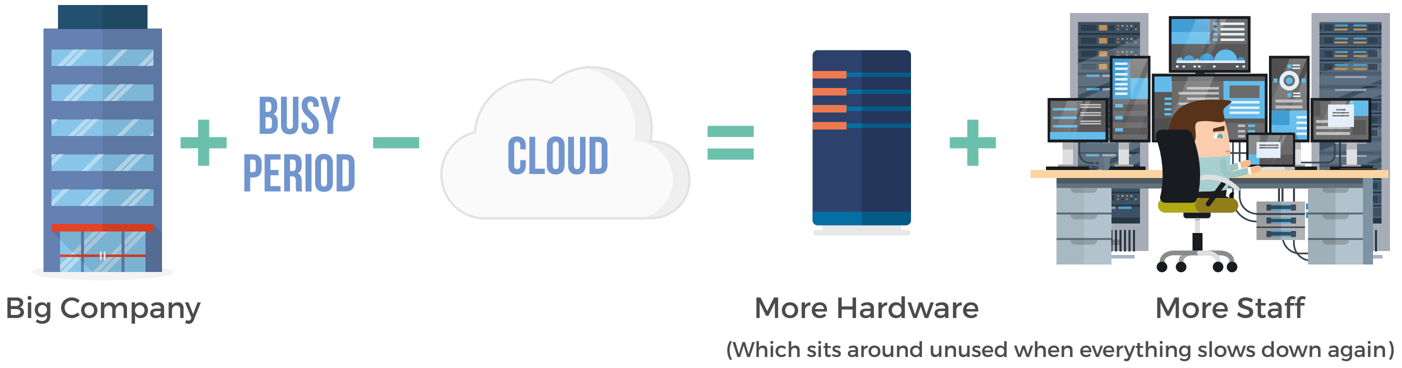
It lets you:

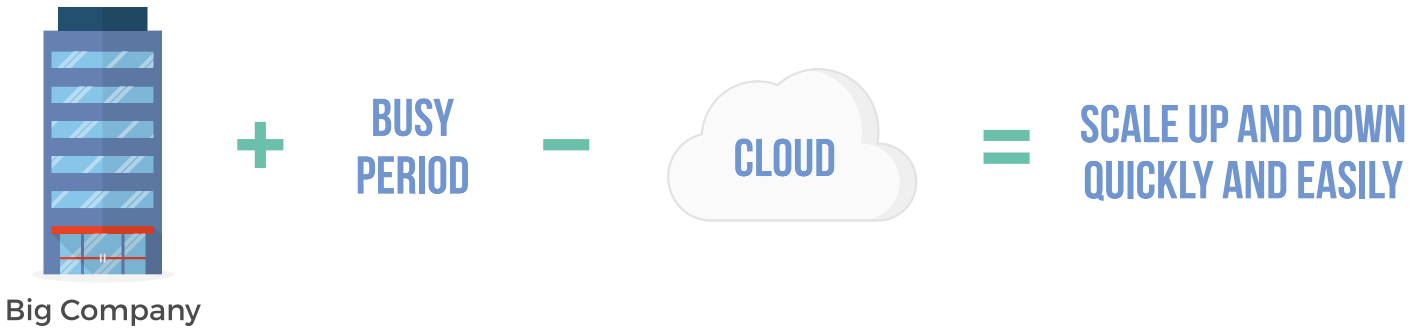
- Manage a lot of things yourself, where you would previously have needed human interaction
- Cut costs
- Reduce your requirements for physical servers

Back in the day, there was a single server to run every application. As a result, the places that held data needed to be bigger, and the hardware ran hotter and needed considerable cooling.

Now, with Cloud technology, we've got a more compact, efficient way of storing and accessing data.

One good way to look at how the Cloud works is like this:





TAKEAWAY

The Cloud is a newish form of data storage that's often easier and cheaper to manage.

TYPES OF CLOUD MODELS

The types of Cloud you're likely to run into can be split into 3 deployment categories and 3 service categories:

Cloud Deployment Models

Public Clouds

A public Cloud is completely hosted on external servers, and support comes from the provider.

Virtually anyone can become a customer and gain access to the resources hosted on a public Cloud.

This method is highly scalable, which makes it ideal for start-ups or individuals that don't have the resources or the need for a private Cloud of their own.

This Cloud deployment model is characterized by its multitenancy. That means since virtually anyone can become a customer, there's a diverse client base where clients are mostly unaware of each other.

This type of Cloud model is dependent on the quality of the third-party provider, meaning the provider must take security seriously. They're responsible for protecting all of their tenants equally.

This means support costs may be high and the customer has little control over other tenants, hardware upgrades, and physical/cyber security. Customers need to be able to trust their provider to feel confident in having their data on a Cloud with public access.

Private Clouds

Private Clouds are internally owned and managed by the customer or company.

This gives the customer total control over hardware, upgrades, and security without having to entrust a third party to be legally sound.

With more control, though, comes more responsibility. Using a private Cloud model means that costs are higher based on the need for more experts, training, and internal support. Without investing in the IT support for a private Cloud, the security of that Cloud is at risk.

BONUS FACT! There's also a more obscure type of private Cloud called a community Cloud.

The community Cloud model is owned by multiple organizations instead of just one.

This model is used primarily by research groups, government agencies, and partnerships between companies.

Hybrid Clouds

A hybrid cloud connects private and public Cloud operations.

It's not as popular as the public or private models are right now, but hybrid clouds are quickly becoming embraced more widely as the future of Cloud computing.

This kind of deployment allows the user more control in some areas, because it has the flexibility of a private Cloud, with the benefits of scalability and overall cost savings of a public Cloud.

Cloud Service Categories

Infrastructure as a Service (IaaS)

Infrastructure as a Service can be thought of as the foundation of Cloud services.

This service provides consumers with computing resources they can build on.

IaaS allows clients to build a virtual infrastructure with pooled resources, which means loads of stretchiness in terms of size.

What used to require a large amount of physical hardware and space now only requires enough hardware to access these shared resources.

Cloud providers can facilitate measured service to create the appropriate size and configurations of an infrastructure based on what the consumer's specific needs are.

Examples of IaaS include: Amazon Web Services (AWS) and Oracle.

Platform as a Service (PaaS)

Platform as a Service is the next layer above the IaaS foundation layer. Sounds like some Star Trek stuff.

Platforms are usually offered alongside Software as a Service (SaaS) and, in such cases, the platforms are built to support the software.

Examples of PaaS include: Google App Engine, Windows Azure, and AWS Elastic Beanstalk

Software as a Service (SaaS)

Software as a Service is the roof to our Cloud computing house. SaaS functions on top of a platform and is usually charged monthly or on a per use basis.

Examples of SaaS include: Microsoft 365, Google Docs, and Salesforce.

TAKEAWAY

Three Cloud deployment models: Public, Private (and community) and Hybrid.

Three Cloud service categories: Infrastructure (IaaS), Platform (PaaS) and Software (SaaS) as a service.

CLOUD STRIFE – RISKS

According to cyber-risk analytics firm Cyence and the insurer Lloyd's of London, the damage the 2017 WannaCry virus caused could have potentially reached $53 billion in less than a week, if they'd have carried out a world-wide hit on Cloud-based businesses.

Luckily, it only spread to over 150 countries, and only cost a few billion.

A FEW BILLION.

Just goes to show that the risks of Cloud computing are serious.

Because there are so many benefits to the Cloud, sometimes people rush into it, without taking the time to consult properly with security experts and their IT departments.

This leads to data breaches and weak access management – two of the biggest Cloud computing threats according to the Cloud Security Alliance.

In fact, there was a data leak of over 200 million US voter records in 2017. According to a cyber-risk analyst, the leak occurred because one of the contractors who set up the Cloud account set the Amazon Web Services S3 storage bucket files to public permissions, rather than private.

Basically, somebody messed up – human error.

The data was exposed because the contractor didn't have any monitoring mechanisms in place for their externally-facing systems.

It can happen to anyone. Which is why it's so important to consult with experts when setting up Cloud Computing, and running regular checks.

However, there's more to Cloud computing risks than just human error.

For example...

- Loss or theft of intellectual property
- When a Cloud service is breached, cyber criminals can gain access to sensitive data. Even without a breach, certain Cloud services can even pose a risk if their terms and conditions claim ownership of the data uploaded to them.
- Compliance violations and regulatory actions
- These days, most companies operate under some sort of regulatory control of their information. Under these mandates, companies must know where their data is, who is able to access it, and how it is being protected. Cloud computing can often violate these tenets.
- Loss of control over end user actions
- Imagine a salesperson, about to resign, who downloads a report of all customer contacts, uploads it to a personal Cloud storage service, and then accesses it once employed by a competitor. If you're not on top of things, you mightn't find out until it's too late.
- Malware infections that unleash a targeted attack
- Cloud services can be used as a vector of data exfiltration. Some attackers encode sensitive data into video files and upload them to YouTube. There's also malware that exfiltrates sensitive data via Twitter accounts. Phishing attacks can also be used.
- Contractual breaches with customers or business partners

- Contracts among business parties often restrict how data is used and who is authorized to access it. When employees move restricted data into the Cloud without permission, business contracts may be violated.
- Diminished customer trust
- Data breaches result in customers and clients trusting you less. Cyber-criminals stole over 40 million customer credit and debit card numbers from the retail giant Target, which led to a drop in their sales.
- Data breach requiring disclosure and notification to victims
- If sensitive or regulated data is put in the Cloud and a breach occurs, the company may be required to disclose the breach and send notifications to potential victims. General Data Protection Regulation (or GDPR) requires this, for instance. Regulators can levy fines and consumers often file lawsuits.
- Increased customer churn
- If customers suspect their data isn't fully protected, they might take their business elsewhere.
- Revenue losses

When the store Target had a data breach, there was a 46% drop in the company's quarterly profit – ultimately cost $148 million. As a result, the CIO and CEO resigned.

CLOUD STRIFE – RISKS

According to a Cloud study, 64% of respondents say their companies can't confirm if their employees are using their own Cloud in the workplace.

To reduce the risks of unmanaged Cloud usage, companies first need visibility into the Cloud services in use by their employees. They need to understand what data is being uploaded to which Cloud services and by whom.

With this information, IT teams can enforce corporate data security, compliance, and governance policies to protect corporate data in the Cloud.

Accordingly, the two most important steps in switching over to Cloud computing are these:

1. The proper implementation of security measures, and
2. Access to qualified cybersecurity advisory personnel

Make sure you put these into practice if you have, or are considering, Cloud solutions.

TAKEAWAY

There are many risks when it comes to Cloud Computing. The best thing you can do to keep yourself safe is use IT experts to help you set up and manage your Cloud usage safely and effectively.

QUIZ

Okay, you've done a lot of reading there. Here's a few questions to make sure it's sunk in. Sunken? Sonk?

Whatever. Answer these. Go back and look it up if it helps – it's about information retention, not your score.

1. What is the Cloud again? And what's it good for?

____

____

2. What are the 3 types of Cloud Deployment models and Cloud Service categories.

____

____

3. What are some of the biggest risks related to Cloud computing?

____

____

4. What are the key things worth bearing in mind when setting up and using Cloud computing?

____

____

SUMMARY

The Cloud has lots of benefits, but also plenty of risk.

It's getting used more and more, by governments, businesses, and other organizations, but that can just mean more danger of data being misused.

The best way of avoiding the pitfalls and maximizing the benefits are to create models that are complete regarding cost, efficiency and security.

If that doesn't sound like something you can do yourself, there's no shame in asking for a little help.