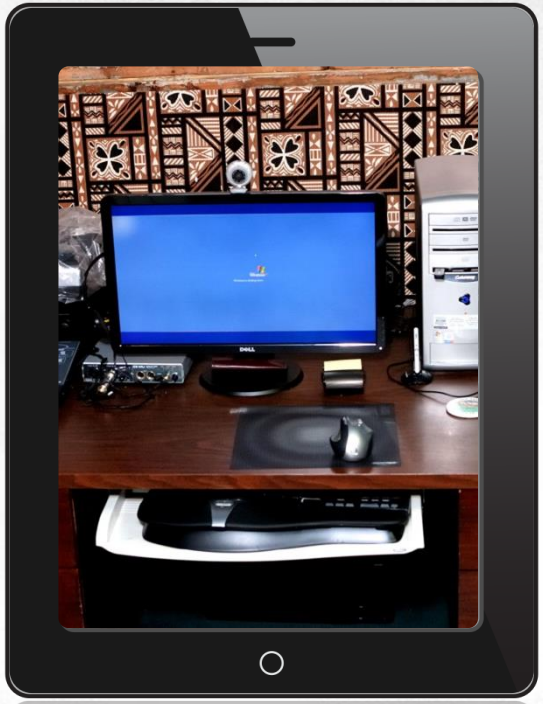
RISK ASSESSMENT

INTRODUCTION

THE MOTIVATION FOR MOST LAUNCHED ATTACKS IS TO ATTAIN A FINANCIAL PROFIT

The lower the cost of an attack, the higher the profit for the attacker. It is also directly proportional to the number of people within the attack impact zone

Before you secure a computer system, profile gains and losses comprehensively

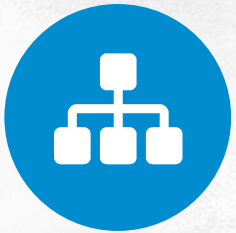


INTRODUCTION

Here's a basic simulation of gains and profits of not having a good anti-virus protection. Assumptions:

The average annual salary of an employee is 100,000 USD

There are 260 working days per year



Removing viruses from a workstation takes roughly 2 hours

INTRODUCTION

Here's a basic simulation of gains and profits of not having a good anti-virus protection. Assumptions:

Two employees participate in this procedure (an IT staffer and the person working at the compromised computer)

$$\frac{100000}{260\text{days}} \times \frac{2\ \text{persons} \times 2\ \text{hours}}{8\text{-hourshift}} = 192\$$$

Divide salary value by working days and multiply the result by the downtime. The result is your internal cost of removing viruses from one host.

Let's say your computer system has 500 workstations

INTRODUCTION

Here's a basic simulation of gains and profits of not having a good anti-virus protection. Assumptions:

Let's assume only 5% will become compromised in a month

$(500 \times 5\%) * 192 = 4807\$$

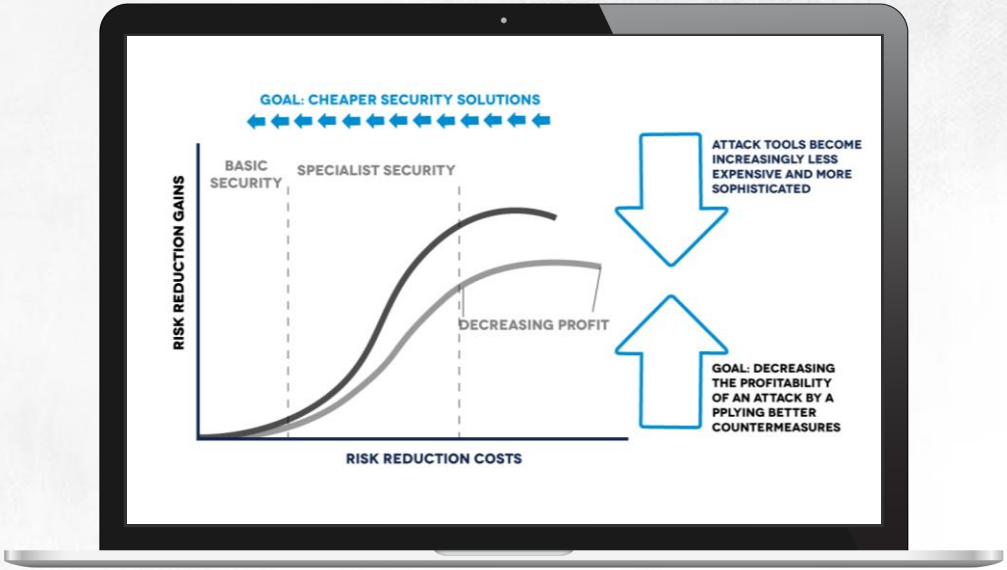
A single recovery operation should be multiplied by the monthly number of occurrences. The result is your internal monthly cost of removing malware from a computer system:

Let's say your computer system has 500 workstations

GAINS AND LOSSES

YOUR GOAL IS TO SECURE A COMPUTER SYSTEM

in such a way that your risk reduction investments force attackers to put in more effort and money into trying to break into your system



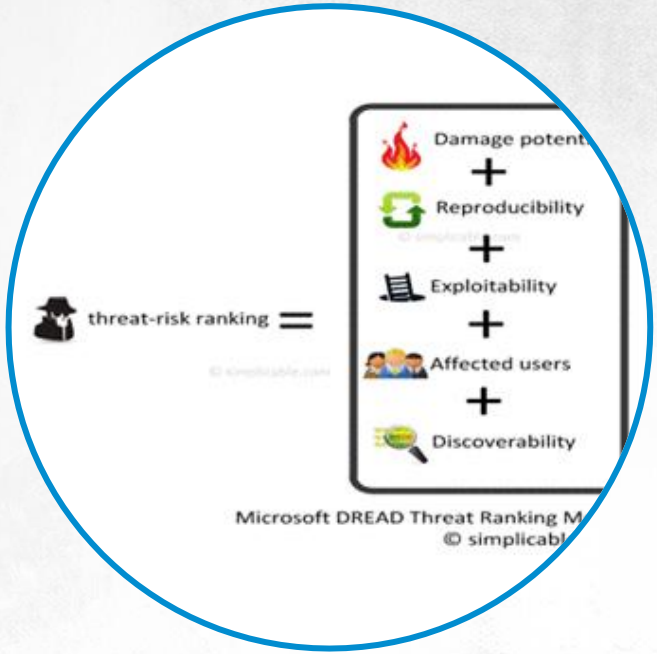
RISK ASSESSMENT MODEL

DREAD

THE DREAD MODEL PROVIDES A GOOD FRAMEWORK FOR RISK ASSESSMENT FOR MOST CASES

It defines five categories that have the biggest effect on assessing potential risks:

- Damage potential
- Reproducibility
- Exploitability
- Affected users
- Discoverability

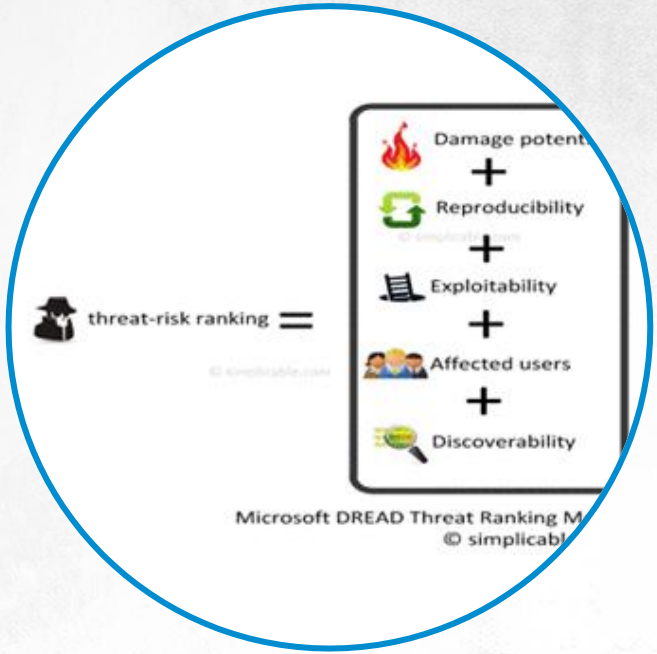


RISK ASSESSMENT MODEL

DREAD

EACH CATEGORY IS GIVEN AN ESTIMATED rating in the model. The ratings are then summed and divided by the number of categories
The result is the estimated probability of a risk

MODELLING POSSIBLE THREATS (for example using STRIDE) and assessing risks will enable you to take up economically justifiable steps to mitigate your losses and prioritize and create a proper sequence for security measures



DREAD

Damage potential

TO ASSESS THIS RISK, ANSWER THIS QUESTION: What direct and indirect losses can be caused by the damage and loss of a resource?

LIKE ANY OTHER CATEGORY, DAMAGE POTENIAL MAY TAKE THESE RATINGS:

- Small, rating 0
- Medium, rating 5
- High, rating 10

DREAD

Reproducibility

TO GET ASSESS THE RISK FOR THIS CATEGORY, ANSWER THIS QUESTION: HOW EASY IS IT TO REPRODUCE THE ATTACK?

- If although a given vulnerability is well-documented, it is hard to reproduce the attack, the risk should be given a rating of 0

DREAD

Reproducibility

- If reproducing the attack requires the reoccurrence or repeating of a specific situation (for example program settings) or requires the attacker to take up additional operations, the risk should be given a medium rating of 5

- If it is incredibly easy to automate the attack and it doesn't require the attacker to perform any additional operations or have specialist knowledge, it should be given a high rating of 10

DREAD

Exploitability

DREAD

Exploitability

THIS IS THE MOST COMMON RISK CATEGORY PEOPLE CONSIDER, AND MAY BE ASSESSED BY ANSWERING THIS QUESTION: HOW EASY IS IT TO LAUNCH THE ATTACK?

- If to launch it, you'd require specialist knowledge, large budget or obscure tools, exploitability should be given a rating of 0
- If it's easy to find guidelines on exploiting the vulnerability online or if tools that exploit it can be created using widely-available software like Metasploit, exploitability should be given a medium rating of 5
- If to launch the attack, the attacker doesn't need specialist knowledge and the needed tools are either already developed or easy to create, exploitability gets a rating of 10

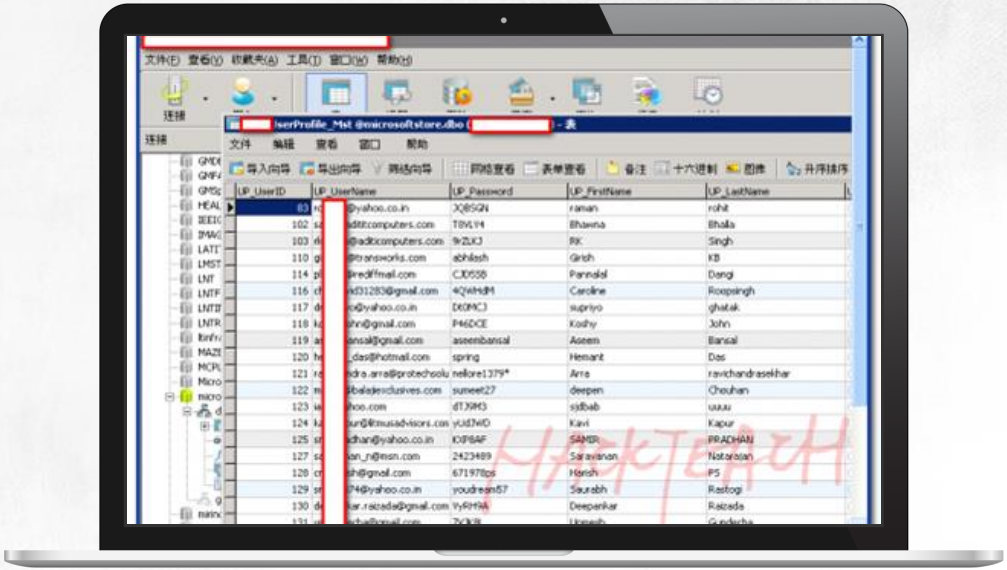
The risk of exploitability increases proportionally with the time elapsed since a vulnerability was first detected

DREAD

Affected users

THIS CATEGORY IS USUALLY GLOSSED over by smaller IT teams. However, even a minor problem, if it is affecting tens of employees or more may turn into a disaster pretty quickly.

TO ASSESS THIS RISK, ANSWER THIS QUESTION: How many people will be unable to work if the attack is successful?



DREAD

Affected users

If the problem impacts all or most users, give it a rating of 10

If the problem impacts from 10 to 25% of users, for example everyone who uses a specific version of the OS or a program running with non-standard settings, Affected users should be given a medium rating of 5

If the problem impacts a negligible group of users (several per cent), for example only admin-level users or personnel using a non-standard, non-default program function, the risk should be given a rating of 0

DREAD

discoverability

THE FIRST QUESTION you have to answer if an attack is successful is about the resources that could have been accessed and affected.

TO ASSESS THIS RISK, answer this question: How easy is it to discover the attack?

DREAD

discoverability

IF THE ATTACK IS DETECTED

immediately after it's launched, for example there is a significant CPU usage increase in affected computers or you can see some files and folders have been deleted or hidden, give this element a rating of 0

IF THE ATTACK RESULTS

in strange, non-typical network activity or non-typical (unstable) software operation, discoverability takes a rating of 5

IF YOU'D NEED HIGHLY-SPECIALIZED TOOLS

(like rootkit detectors) to discover the attack, the risk should be given a rating of 10

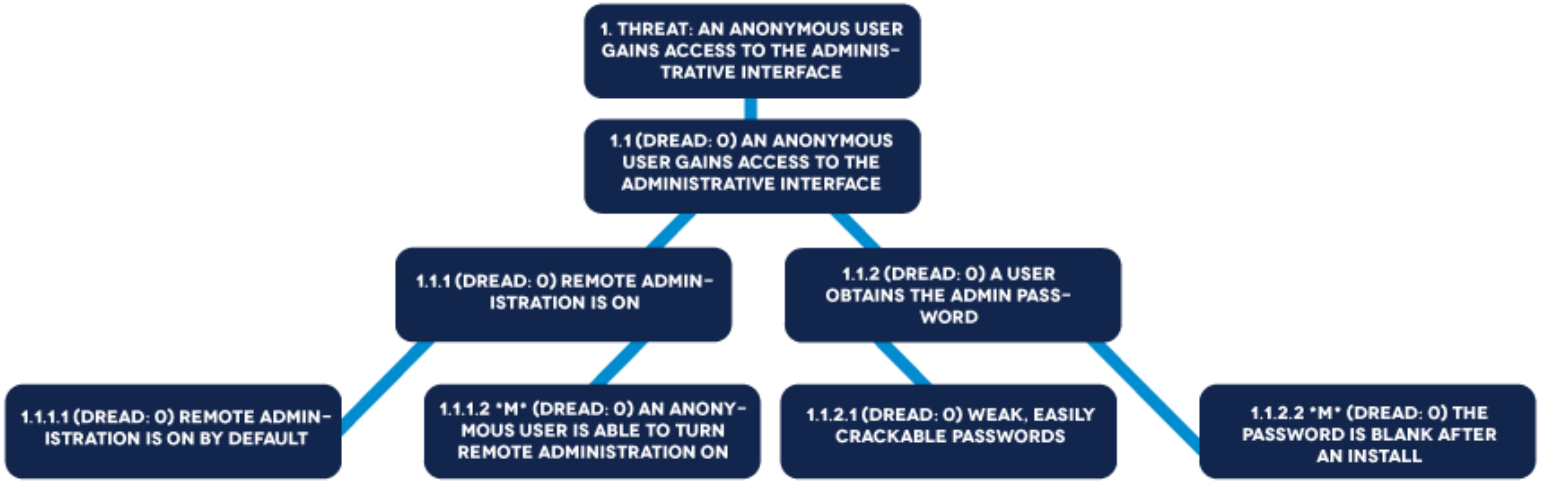
DREAD

Risk Calculator

THREAT	D	R	E	A	D	RISK	PRIORITY
SQL INJECTION USED TO OBTAIN CONFIDENTIAL INFORMATION FROM A DATABASE	10	5	5	10	10	40/5= 8	HIGHEST
INTERCEPTING AUTHENTICATION DATA VIA A MAN-IN-THE-MIDDLE ATTACK TARGETING A HTTPS-PROTECTED WEB APPLICATION	5	10	5	5	0	25/5=5	LOW
A MASS-MAILING VIRUS DELETING USER FILES	5	10	10	10	0	35/5=7	HIGH

DREAD

Risk Assessment: Example

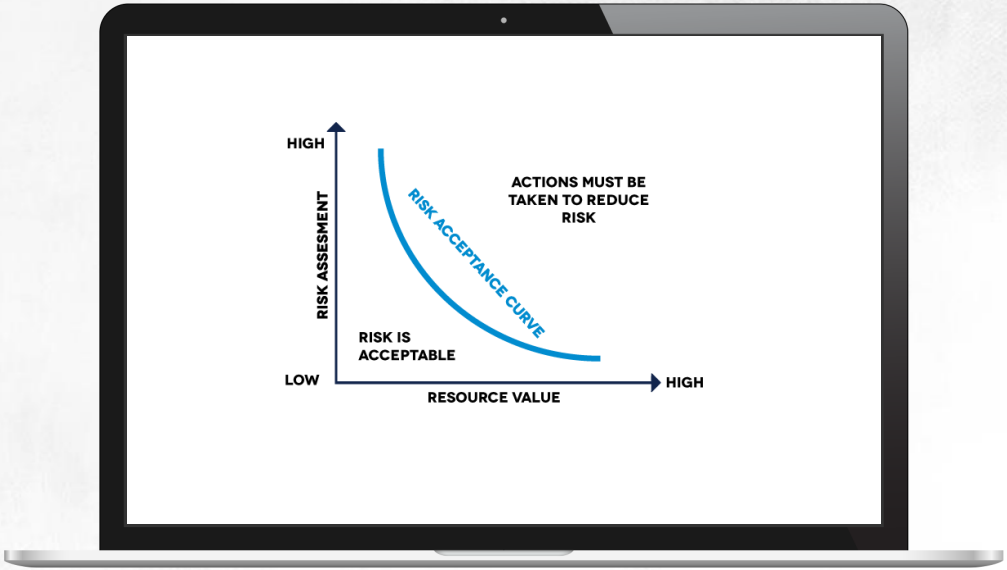


PROTECTION STRATEGIES

Risk Tolerance Curve

KNOWING THE VALUE OF YOUR RESOURCES and prioritizing potential risks allows you to take a more financially-informed decision about the methods you'll use for protecting the resources

FIRST OFF, SEE IF YOU CAN ACCEPT a given risk threshold or if you are willing to take up steps to mitigate the risks and protect the resources

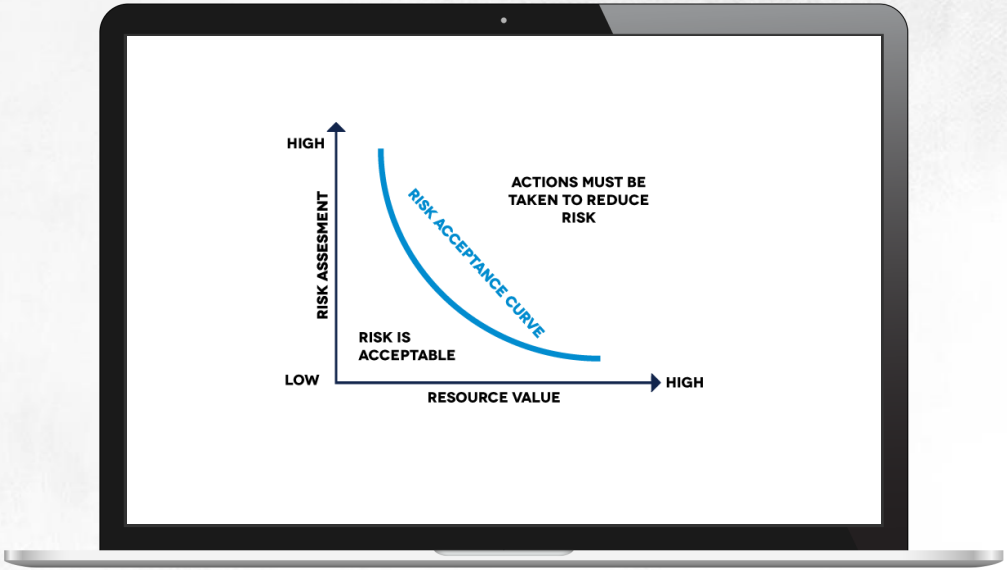


PROTECTION STRATEGIES

Risk Tolerance Curve

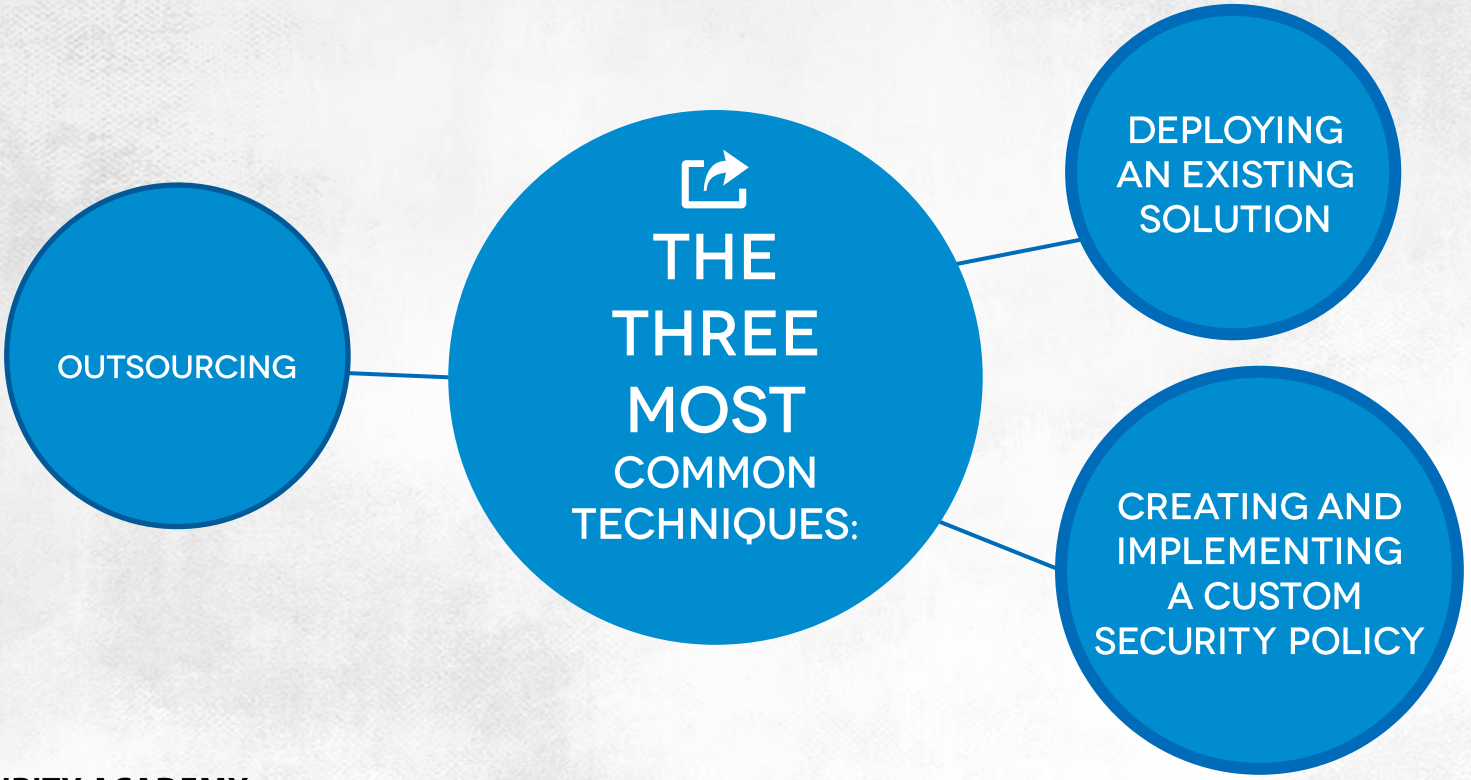
THE DECISION TO REDUCE A RISK DEPENDS on the risk's placement in the chart you can see:

- Below the curve, the risk is acceptable, but you may still take some actions towards minimizing potential damage
- If it is above the curve, you need to take an action to minimize the risk



PROTECTION STRATEGIES

Risk Minimizing Techniques

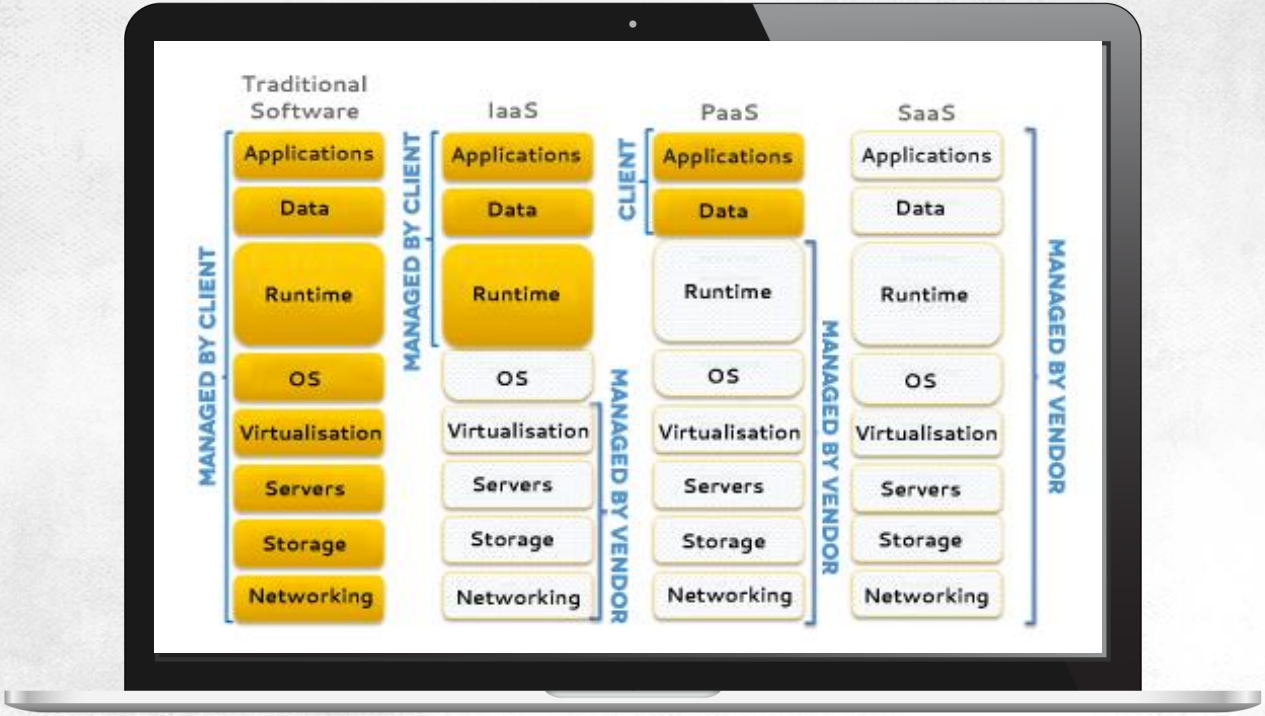


PROTECTION STRATEGIES

Risk Minimizing Techniques

	RISK ACCEPTANCE	OUTSOURCING	EXISTING SOLUTION	INTEGRATED SOLUTION
PROS	LOW COSTS (AT THE OUTSET...)	SLA GUARANTEES FORESEEABLE COSTS	VENDOR SUPPORT	LOW RISK FULL CONTROL
CONS	HIGH RISK NO CONTROL	SMALL CONTROL	INCOMPLETENESS VENDOR DEPENDENCY	HIGH COSTS

CLOUD SECURITY



CLOUD SECURITY

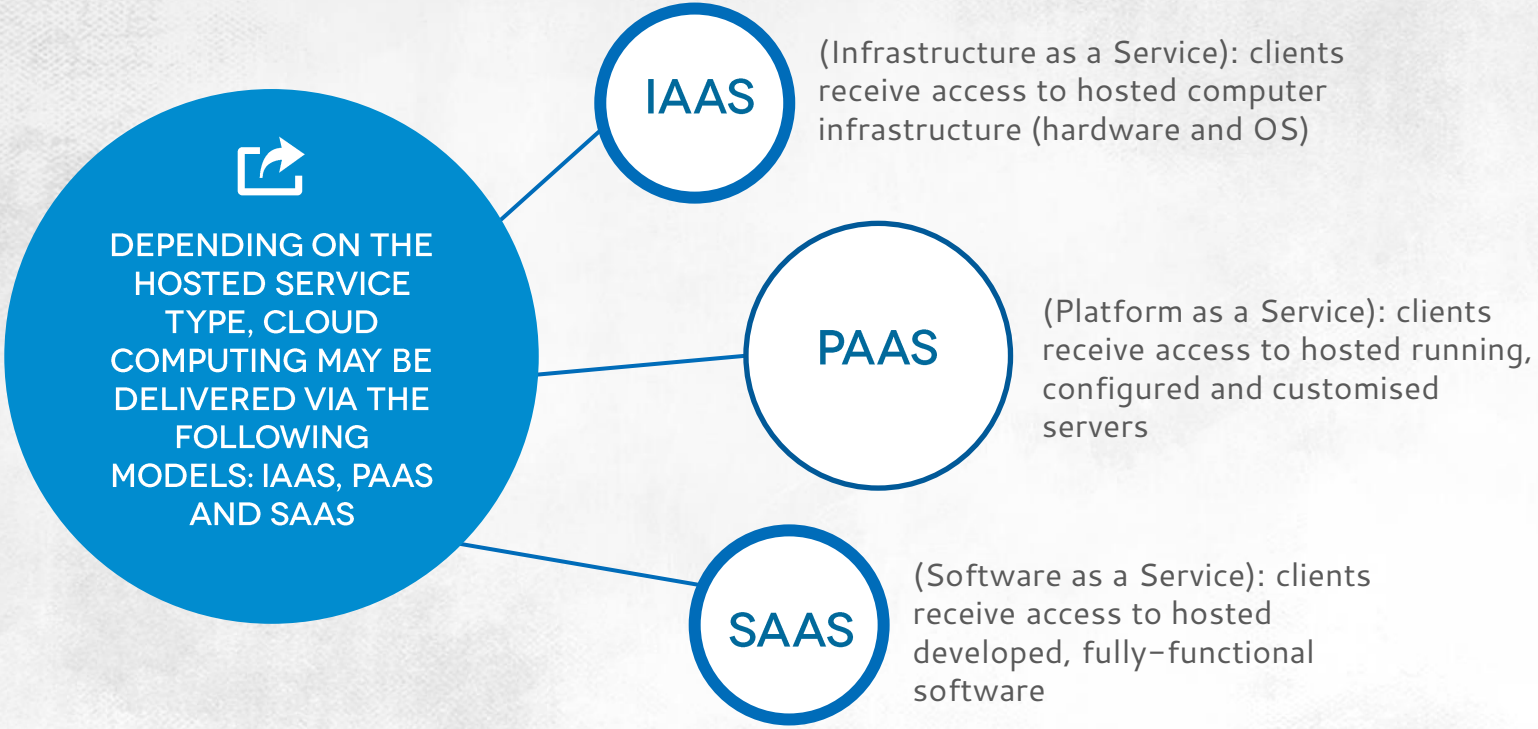
CLOUD COMPUTING RELIES ON USING another company's computer infrastructure, service or program (usually at a fee)

INSTEAD OF SPENDING MONEY TO purchase and maintain its own computer systems, cloud computing allows a company to purchase needed services from an external provider

A PUBLIC CLOUD is available to everyone

PERSONAL CLOUDS are created with a specific client in mind

CLOUD SECURITY



THANKS