Monetising Security as a Managed Service

Microsoft Crayon

Cyber Crime and SMBs; The Facts

Australian Cyber Security Centre (ACSC) – part of the Australian Signals Directorate (ASD)

A cybercrime is reported **every 6 minutes**, on average.

The average self-reported **cost of cybercrime** to **businesses increased** by **14% per cent**.

- **$46,000** for **small business**
- **$97,200** for **medium business**
- **$71,600** for **large business**

What the ACSC considers an SMB

- Sole trader: 1 employee
- Micro business: 2-4 employees
- Small business: 5-19 employees
- Medium business: 20-199 employees

- There has been a 23% increase in cybercrime reported since last financial year
- In the last ACSC SMB survey of almost 2,000 businesses 62% experienced a cyber crime incident
- 1 in 5 SMBs did not know the term “Phishing”
- Half of all SMBs rated their Cyber Security knowledge as average to below average
- 80% of SMBs rated Cyber Security as important to very important
- SMBs that outsourced IT security believe they are better protected than they really are
- Almost half of SMBs reported they spent less than $500 on cyber security per year.

ACSC Annual Cyber Threat Report 2022/2023

Why monetise & package Security as a Managed Service

Example of what MSP's are charging Example 1

PER USER MONTHY Service Packages	SILVER $130	GOLD $160	PLATINUM $210
MANAGED SERVICES			
24x7x365 Remote Support	✔	✔	✔
Ticketing System	✔	✔	✔
Desktop Support	✔	✔	✔
Onsite Support *	✔	✔	✔
Continuous System Health Checks	✔	✔	✔
Backup as a Service		✔	✔
DR as a Service		✔	✔
BCP as a Service		✔	✔
Annual BCP Testing		✔	✔
Monthly IT Report		✔	✔
Microsoft 365 Licenses (Business Standard)		✔	✔
Cyber Security Report		✔	✔
Mobile Device Management -			✔

Example 1 continued

CYBER SECURITY			
Network Monitoring	✔	✔	✔
Dark Web Monitoring	✔	✔	✔
Endpoint Protection		✔	✔
Anti-Virus		✔	✔
Anti-Malware		✔	✔
Anti-Phishing		✔	✔
Ransomware Protection		✔	✔
Email Security		✔	✔
Web Security		✔	✔
Cloud Protection		✔	✔
Network Security			✔
Detection & Response			✔
Automatic Threat Remediation			✔
VALUE ADDED SERVICES			
Quarterly IT Strategy Meeting			✔
Annual IT Budget			✔
Vendor Management			✔
2 Hour Service Level Agreement			✔
Managed Cyber Security			✔

Example 2

YOUR MANAGED IT SERVICE PACKAGES

All our plans include infrastructure monitoring and unlimited remote IT support. We look after you by stopping issues before they happen and getting you back up and running fast. That's why we have a 4.7 out of 5 customer satisfaction rating.

Essentials	Business	Premium
The essentials you need to stop your IT headaches with unlimited remote support.	Keep your business ticking with 24/7 support, best-of-breed software, and strong technology governance * Minimum plan required for Cyber Insurance.	On top of our best-in-market IT services, leverage optimyze's Virtual CIO and our training programs to drive your business forward.
$125 Per user Per Month	$165 Per user Per Month	$195 Per user Per Month
Essentials Includes:	**Everything in Essentials, PLUS:**	**Everything in Business, PLUS:**

User Support:

- Unlimited Remote Support
- Unlimited On-Site Support

Business Productivity Tools:

- 365 Business Premium License

Proactive Maintenance:

- Computer Patching and Updates (all software)
- Device Health Monitoring
- Device Performance Optimization
- Network Infrastructure Maintenance

Cyber Security:

- Antivirus Software
- Antivirus Monitoring

IT Management:

- Customer Support Portal
- IT Documentation
- Asset Management
- Monthly Executive Report

User Support:

- Urgent After-Hours IT Support

Business Productivity Tools:

- 365 Business Premium License
- Cloud Print Management

Cyber Security:

- Microsoft 365 Cloud Backup
- Password Manager App
- Endpoint Security Software (EDR)
- Spam and Web Filtering
- Network Intrusion Detection
- Identity and Access Monitoring
- Firewall & Network Monitoring

IT Management:

- Vendor & Supplier Management
- IT Planning & Budgeting
- Cyber Insurance Support
- E-Waste Recycling
- Monthly IT Meeting

Strategic Business Support:

- Access to Virtual vCIO Strategic Planning
- Weekly Onsite Check-ins

Business Productivity Tools:

- 365 Business Premium License
- Cloud Print Management

Cyber Security:

- Dark Web Monitoring
- Continuous vulnerability Monitoring
- Realtime Threat Intelligence
- Behavioural Analytics
- Security Event Analysis
- Cyber Security Awareness Training

IT Management:

- IT Policy Development
- Budget & Financial Mangement
- Compliance & Regulatory Support
- Risk Management

How to monetise & package Security as a Managed Service

Use a Cybersecurity framework to educate your customers & increase your revenue

ACSC- Essential 8

Application Control

Patch Applications

Configure MS Office Macro Settings

User Application Hardening

Restrict Administrative Privileges

Patch Operating Systems

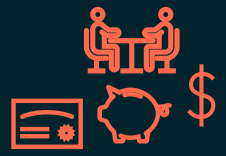
Multi-Factor Authentication

Regular Backups

Crayon

Who is your customer

- What is the right Security Posture for your clients.
- Should you have more than one offering.
- Every client should have a default Basic Security setting. Some clients need more.
- There is no such thing as different flavours of Security.



- Personal Details
- Financial Status
- Transaction Details
- Taxation information
- Share trading App
- B2B with Accountants

- Co Account names
- EFTPOS Machine
- Warehousing App
- Shared mailboxes

What do you pick, what do you add

Control	Control Action	Assumptions & Comments	Licence SKU
Application Control	Block executable mail content. Execution in temp folders. Protect against un-wanted Apps. Restrict ActiveX. App Control W/L.	Defender for Office, MDE ASR rules, MDAC	M365 Bus Premium Defender for Business, Defender for Office P2
Patch Applications	Disable un-supported Apps. Manage Security on Internet facing servers. Review vulnerabilities daily.	Intune, Win update for Bus, Defender for endpoint, MS Edge, Intune.	M365 Bus Premium, Defender for Business, Microsoft Intune Defender for Endpoint P2.
Configure MS Office macro settings	Disable un-necessary Macros. Macros from Internet blocked. Use of Macros	MS Defender for endpoint, MS Defender for office safe-links, ASR	M365 Bus Premium, Defender for Business, Microsoft Intune Defender for Office P1
User Application hardening	Block internet Ads. Restrict web browser processing Java	Intune, Defender Smartscreen, MS Edge managed by Intune.	M365 Bus Premium Defender for Business, Microsoft Intune
Restrict Administrative privileges	Restrict and limit PA access, and PA Internet, services, email, access. Role based PA, Manage PA's. Limit use of roles	Entra ID.	M365 Bus Premium, Microsoft Intune Entra ID P1 & P2
Patch Operating Systems	Update Internet facing servers and run vulnerability scans. Replace un-supported Operating systems.	Intune, Def for endpoint, Win up-date for Business.	M365 Bus Premium, Microsoft Intune Defender for Business
Multi-Factor Authentication	Enable MFA for all users. Enable MFA for third party users	Entra ID.	M365 Bus Premium, Entra ID P1 & P2
Regular Back-ups	Create and retain Back-ups. Back-up policies and procedures.	Azure Back-up, M365 Back-up	Azure Back-up, M365 Back-up

Crayon

Refine, then Market your offer

Control	Control Action	Assumptions & Comments	Licence SKU
Application Control	Block executable mail content. Execution in temp folders. Protect against un-wanted Apps. Restrict ActiveX. App Control W/L.	Defender for Office, MDE ASR rules,	M365 Bus Premium, Defender for Office P2
Patch Applications	Disable un-supported Apps. Manage Security on Internet facing servers. Review vulnerabilities daily.	Intune, Win update for Bus, Defender for endpoint, MS Edge, Intune.	M365 Bus Premium, Defender for Business, Defender for Endpoint P2.
Configure MS Office macro settings	Disable un-necessary Macros. Macros from Internet blocked. Use of Macros	MS Defender for endpoint, MS Defender for office safe-links, ASR	M365 Bus Premium, Defender for Business, Defender for Office P1
User Application hardening	Block internet Ads. Restrict web browser processing Java	Intune, Defender Smartscreen, MS Edge managed by Intune.	M365 Bus Premium
Restrict Administrative privilege s	Restrict and limit PA access, and PA Internet, services, email, access. Role based PA, Manage PA's. Limit use of roles	Entra ID P1.	M365 Bus Premium, Entra ID P1 & P2
Patch Operating Systems	Update Internet facing servers and run vulnerability scans. Replace un-supported Operating systems.	Intune, Def for endpoint, Win up-date for Business.	M365 Bus Premium, Defender for Business
Multi-Factor Authentication	Enable MFA for all users. Enable MFA for third party users	Entra ID P1.	M365 Bus Premium, Entra ID P1 & P2
Regular Back-ups	Create and retain Back-ups. Back-up policies and procedures.	Azure Back-up, M365 Back-up	Azure Back-up, M365 Back-up
User Training	User Awareness and Anti-Phishing campaigns	If not Defender for O365 P2	rhipe can assist you with usecure https://www.usecure.io/en/demo-centre

Crayon

usecure HRM — 4 security products in 1

MSP focused – white labelled – admin light – multi tenant

uLearn

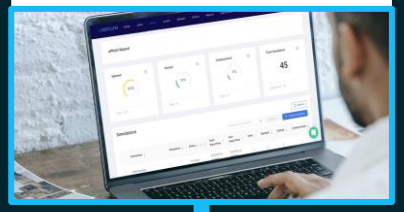
Security Awareness Training

User-Tailored Programs
Compliance Library
Custom Course Builder

uPhish

Simulated Phishing

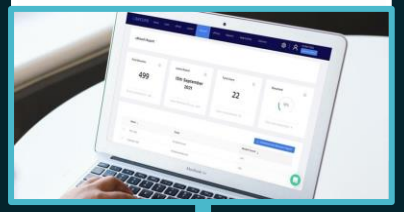
Automated Phishing
Template Library
Custom Spear-Phishing
Message injection



uBreach Starter / PRO

Dark Web Breach Scans

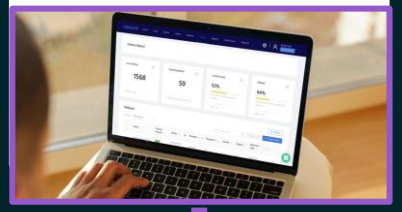
Ongoing Users Monitoring
Breach Dashboard
PRO: Notifications/Reporting
PRO: Domain Monitoring



uPolicy

Policy Management

Trackable eSign Approvals
Template Library
Custom Template Builder



Human Risk Analytics >> Automated Performance Reports

What is a Service Description

End User support per user per month			
Service Description	Silver	Gold	Platinum
24 x 7 Remote Support	✓	✓	✓
Desktop Support	✓	✓	✓
On-site support	✓	✓	✓
Device Patching	✓	✓	✓
System Monitoring and Alerting		✓	✓
System Back-up		✓	✓
Disaster Recovery		✓	✓
Monthly Reporting		✓	✓
Mobile Device Management		✓	✓
Business Continuity			✓
Network Security			✓
Application Patching			✓

Link to description in main body of document

Service Description End User Management main document

Description of Services

Disaster Recovery
Included in the service is a Disaster Recovery service provided by MSP in client's Azure service that captures data of client servers at regular intervals including its data, operating system application and configuration and replicates those images to a secondary Azure data centre, for purposes of restoration of service.

Monthly Reporting
MSP will provide clients with monthly reporting detailing resolved tickets, patching, antivirus performance, service availability and network reliability.

What is a Service Description

End User support per user per month				
Service Description	Silver	Gold	Platinum	Cyber Security
24 x 7 Remote Support	✓	✓	✓	
Desktop Support	✓	✓	✓	
On-site support	✓	✓	✓	
Device Patching	✓	✓	✓	
System Monitoring and Alerting		✓	✓	
System Back-up		✓	✓	
Disaster Recovery		✓	✓	
Monthly Reporting		✓	✓	
Mobile Device Management		✓	✓	
Business Continuity			✓	
Network Security			✓	
Application Patching			✓	
Include or keep separate				
End Point Protection				✓
Email Security				✓
Detection and Response				✓
Auto Threat Remediation				✓
Password and Sign in Management				✓
Monthly Security Reporting				✓
Application Protection				✓
User Awareness Training				✓

Link to description in main body of document

Service Description Cyber-Security main document

Description of Services

End Point Protection

All antivirus licensing is included for Servers, MAC's and PC's. MSP monitors the antivirus software 24/7 and in the event of a virus/ad-ware/spyware etc. being detected a service ticket be created in MSP's ticket management system. MSP will address viruses as requiring an emergency response by a technician to confirm virus removal.

User Awareness Training

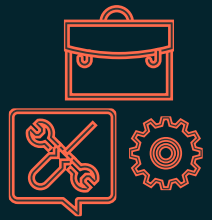
MSP includes and requires all computer users at client to participate in regular security awareness training as provided. Training may include simulated phishing attacks, instruction in company IT policies and best practices, compliance training and testing.

New Security customer

- What do they currently do about Security.
- What is the status of their IT.
- How will we get them to our Security baseline that meets their needs.
- Existing customer question:
  - "What do you think we have you covered for when it comes to Cyber-Security"
  - "What about those questionnaires from your Insurance company, we helped you with"

Security Assessment

- Everything or just endpoints
- Just the results or Analysis too
- Prioritised



Desktop or Tools

- Crayon White Label
- Microsoft Free
- Microsoft Secure Score
- Build your own

Microsoft Free Security Assessments

- QS solutions (the makers of CSAT) collect data to perform the assessment, and the data is subject to GDPR rules prior to it being destroyed, this is important as a client may ask about this.
- The Microsoft Security Assessment Tool (MSAT) is a risk-assessment application designed to provide information and recommendations about best practices for security within an information technology infrastructure.

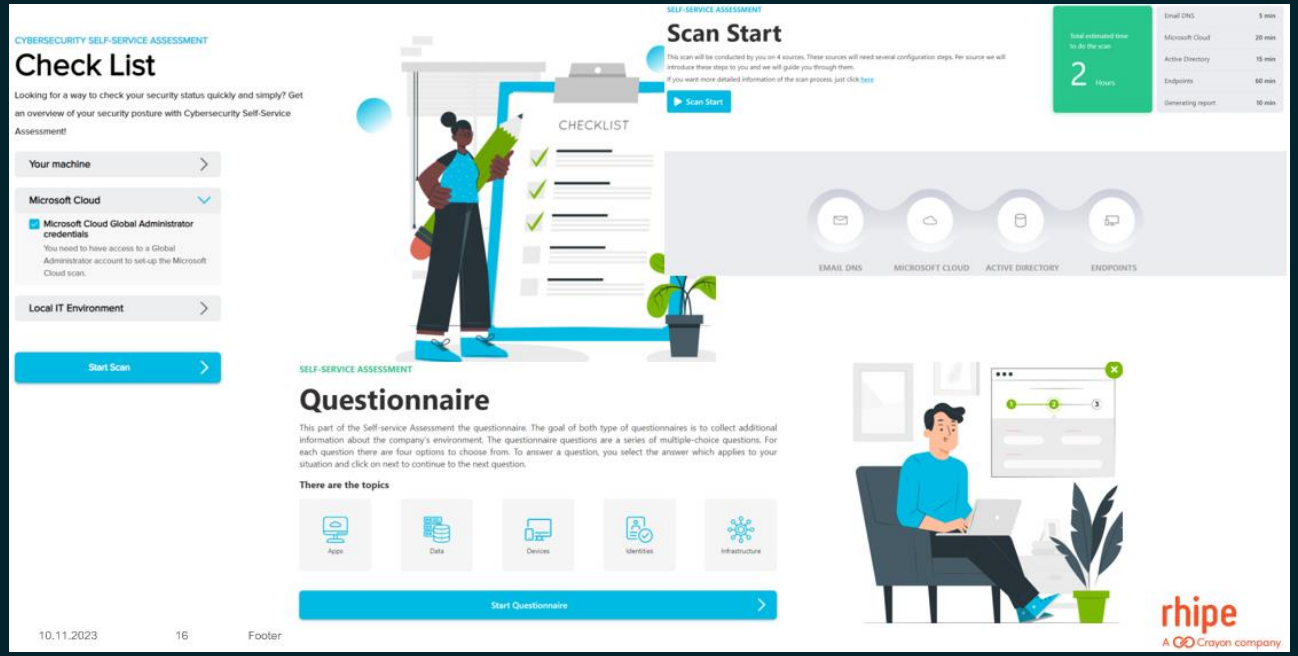
Customer Opportunity: Security Assessments

	CSAT Self Service Assessment	CSAT QuickScan Assessment
Target Group	SMB – Open to all customers	SMB (30-300 Endpoints)
Purpose of Assessment	1. Lead Generation for full-service assessments. 2. Show customers they need a more detailed assessment to identify all cybersecurity risks. 3. Based on a limited number of controls of the Zero Trust Architecture 4. Limited datasets and concise report. Allow for first improvement actions while sparking interest for a full assessment	1. Do a quick check on the cybersecurity hygiene 2. Propose improvement actions based on actual data 3. Quick report and few customizations 4. Based on the CIS controls IG1
Outcomes of Assessment	Positioning of Microsoft's Security solutions in M365 and Azure. Customer will be interested in a comprehensive assessment	Upsell to Microsoft 365 Business Premium, Azure migrations and increase of Azure Consumed Revenue by adding Azure Security
Scan Sources in Scope	• Manual Endpoint Scan of Windows OS • Local Active Directory • Email DNS check • Limited datasets of Microsoft 365 environment • Limited datasets from the Azure tenant • Questionnaire on basic security controls – no official framework	• Basic Automated Endpoint Scan • Local Active Directory • Email DNS check • Microsoft 365 environment • Limited datasets from the Azure tenant • Checked against CIS IG1 (basic security hygiene controls)

Crayon

Aligned to Essential 8

CSAT self service assessment



Here is the link to the Self-Service Assessment Solution Assessment Program (microsoft.com)

CSAT QuickScan assessment

- Microsoft have launched an “SMB Assessment Desk “ who will be supporting the delivery of this assessment

- The SMB Assessment Desk is designed to provide Microsoft’s SMB customers with access to light rapid server migration and cybersecurity-focused assessments using Azure Migrate and QS Solutions’ Cybersecurity Assessment Tool (CSAT), with the goal of providing customer decision-makers and partners with data, insights, and actionable recommendations in support of migration to Microsoft’s cloud services.

- Nominations are via this link https://www.microsoft.com/en-us/solutionassessments/register - then someone from the Microsoft SMB assessment desk will get in touch and kick off process

- Eligibility Criteria: In addition to the number of endpoints (30-300), needs to be customer pre-agreement on assessment, no previous assessment in the same TPID

- Estimated time from nomination approval to report delivery: 1-3 weeks

Use the QuickScan free Assessment FOR 30-300 SEATS

The conversation with the client

Control	Level 0	Level 1	Level 2	Level 3
Application Control				
Patch Applications				
Configure MS Office macro settings				
User Application hardening				
Restrict Administrative privileges				
Patch Operating Systems				
Multi-Factor Authentication				
Regular Back-ups				
User Training				

ASD-8 Security Assessment

- Where are you now the results
- Where does your business need to be
- List, Prioritise and Explain the deltas

- When should the work be done
- How long will it take
- How much will it cost

The conversation with the client

Managed Services Agreement

- Will keep you where you need to be
- 12, 24, 36 months
- On-boarding costs
  - Amortise
  - Upfront
  - Ignore
- Includes assessment if they sign?
- <u>You get a monthly meeting and report</u>

End Point Protection				✓
Email Security				✓
Detection and Response				✓
Auto Threat Remediation				✓
Password and Sign in Management				✓
Monthly Security Reporting				✓
Application Protection				✓
User Awareness Training				✓

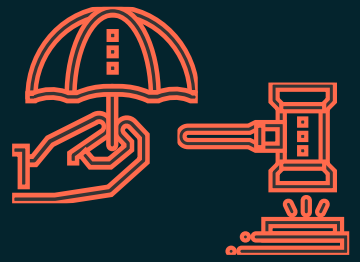
Our MSA includes Cyber-Security

Monthly client Security meeting

Managed Security Service Report

- Show the value of your service
- Agree on what needs to be addressed
- Send in advance of the meeting

Risk Status Report



- Who's risk? Yours or the Clients
- Document it and share with Client
- Show it every month

Our MSA includes Cyber-Security

Report pdf

Why is it so useful

Reports in Microsoft Defender for Business | Microsoft Learn

Monthly Security Summary

May 8, 2023 11:49:19 PM
Report is for the last 30 days: April 8, 2023 to May 8, 2023

Summary

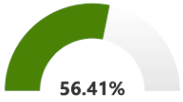
A snapshot of your organization's protection state powered by Microsoft Defender for Business. This report shows how well your organization is prepared to prevent and respond to cyberthreats.

Your secure score is 56.41% and it dropped by 0.22% from last month.It is 9.89% higher than than other organizations of a similar size.1 devices were onboarded this month.0 URLs were blocked across 0 restricted categories.There have been 0 resolved incidents and 0 resolved alerts this month.

Microsoft Secure Score

You have good protection against cyberthreats

Your organization's overall cybersecurity strength has **dropped by 0.22%** since last month.
A higher number indicates more recommended actions have been taken,
which minimizes your risk from attacks.



Your secure score compared to organizations of a similar size

Your score is 9.89% higher than other organizations

Your score	**56.41**/100
Organizations of a similar size	**46.52**/100

Devices onboarded to Defender for Business

1 devices are onboarded

Devices onboarded this month	Devices not yet onboarded
0	**0**

Protection against specific types of threats

Phishing protection hasn't changed
Ransomware protection dropped by 2.24%

Attack name	Your score
Phishing protection	**79.26%** (0%)
Ransomware protection	**47.51%** (-2.24%)

Web content monitoring and filtering

0 URLs blocked

User clicks blocked by category

Leisure	Adult content	Legal liablity	High bandwidth	Uncategorized
0	**0**	**0**	**0**	**0**

Tracked severe suspicious or malicious activities

0 incidents and 0 alerts were resolved

All active incidents	All active alerts
0	**0**

Risk Status report

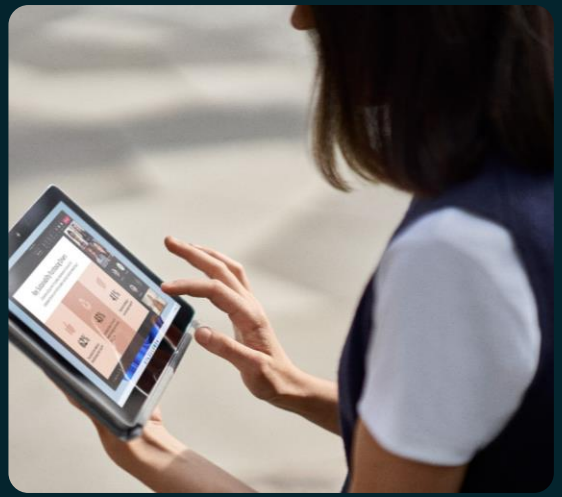
Why is it so important

Risk Status Report for Jedi Engineering

Case No	Risk Title	Description	Notification Date	Client informed	Client Accepts	Comments and Date
17	Application Whitelisting disabled	End user are not happy with restrictions as they believe it is impacting productivity	29/11/2023	Yes	Yes	29/11/23 Client will raise the issue at the next Executive Management meeting, in time for next Security Service meeting
16	Admin Accounts are un-restricted	Certain Executives said they need to make changes on the M365 tenant if their team members have problems, because IT is too slow to respond.	19/09/2023	Yes	Yes	19/09/23 Client will raise the issue at the next Executive Management meeting, in time for next Security Service meeting. 29/09/23 Issue resolved Management agreed only Whiz IT are allowed to make changes

Let’s summarise – Why Microsoft 365 Business Premium

- Here are the benefits



Comprehensive and easy to use

- One solution for productivity and security
- Cloud platform simplifies deployment
- Gets you up and running quickly

Reduces costs

- Eliminates costs of multiple point solutions
- Reduces helpdesk costs
- Eases licensing complexity

Enterprise grade technology

- Integrated security; trusted by enterprises
- AI-powered threat intelligence
- Top rated security vendor

Next Steps

1. Draw up your Security Baseline

2. Translate your Baseline to a Service Description

3. Use the Summary report in Secure Score to make your own monthly client report

4. Make a Risk Register

5. Review the Free CSAT Security Assessments
    1. Self-Service Assessment Solution Assessment Program (microsoft.com)
    2. QuickScan Assessment - Nominations are via this link https://www.microsoft.com/en-us/solutionassessments/register - then someone from the Microsoft SMB assessment desk will get in touch and kick off process

6. Install Microsoft Business Premium into your own tenant and start to use this. Learn how to configure this correctly so come to our next Workshop!!