# Solace Cyber

# Cyber Security Risk Assessment

**LEADERS IN
INCIDENT RESPONSE**

◆ Solace Cyber

# CYBER SECURITY ASSESSMENT SCORE  <span>34%</span>

| Assessment Area | Why it matters | What your score means | Your Score |
|---|---|---|---|
| **External Vulnerability Assessment** | These vulnerabilities are the front doors for attackers to enter your business | 20 of your devices are vulnerable (2 critical, 5 high, 19 medium) | 40% |
| **Phishing Risk Assessment** | Employees can be the weakest link and bypass perimeter security measures. | None of your 30 users clicked on the phishing link | 100% |
| **Microsoft 365 MailFlow Protection** | Mail flow protection can prevent malicious emails arriving in users' inboxes. | Some available protection features are not configured or disabled | 35% |
| **Microsoft 365 Secure Score** | Microsoft's own scoring mechanism provided a good baseline security posture. | Some recommended configuration steps have not been taken | 18% |
| **Microsoft 365 Forensic Audit** | 70% of customers checked with the Solace Cyber CSIRT forensic code had a historical compromise they were unaware of. | We have not assessed your audit data | 0% |
| **MFA Assessment** | MFA requires the use of a phone app or SMS in addition to your username and password, greatly reducing the risk of compromise. | 8 administrators & 50 users do not have MFA enabled | 35% |
| **Backup and Disaster Recovery** | Air gapped backups and a mature DR plan give you the ability to recover from a breach quickly. | Your backup and DR plan may not allow you to recover quickly from a breach | 20% |
| **Remote Worker Security Review** | Secure remote working is essential to prevent cyber-attacks that target remote workers | Refer to Remote Worker Security Review for guidance | 25% |
| **Firewall Review** | A poorly configured firewall won't be as effective at preventing attacks. | Some of your firewalls require security patching | 40% |
| **Cyber Insurance** | Failure to comply with all T&Cs of insurance policy can void it. | We have assessed you against a generic cyber insurance policy | 47% |

# 1 EXTERNAL VULNERABILITY ASSESSMENT    40%

Cyber attackers will be executing scans and reconnaissance against your organisation. Once they find vulnerabilities, they will look to exploit them to gain access to your network. The external vulnerability assessment provides the visibility to know about these gaps first and remediate them before they are exploited. In additional to the cyber security risks this service can identify it is also worth noting that if a breach enters on a device with Critical or high vulnerabilities that is not patched cyber insurance can be void.

## 1.1 EXTERNAL SCAN SCOPE

The following addresses were included within the scope of the scan:

- x.x.x.x
- y.y.y.y
- z.z.z.z/28
- test.co.uk
- a.a.a.a/28
- Test1.com

## 1.2 EXTERNAL SCAN RESULTS

A scan was conducted against your public IP addresses and domains on 06/10/2021. A total of 113 vulnerabilities were detected against the discovered hosts:

| Severity | Score |
|---|---|
| Hosts with Critical vulnerabilities | 2 |
| Hosts with High vulnerabilities | 5 |
| Hosts with Medium vulnerabilities | 19 |

## 1.3 TOP 10

**The top 10 vulnerable hosts are listed below:**

| Host | Critical | High | Medium |
|---|---|---|---|
| x.x.x.x - IP address | 1 | 2 | 11 |
| x.x.x.x | 1 | 1 | 7 |
| x.x.x.x | | 1 | 6 |
| x.x.x.x | | 1 | 9 |
| x.x.x.x | | 1 | 15 |
| x.x.x.x | | | 5 |
| x.x.x.x | | | 6 |
| x.x.x.x | | | 3 |
| x.x.x.x | | | 4 |
| x.x.x.x | | | 9 |

Detailed results of the vulnerability assessment have been provided in the Cyber Security Risk Assessment annex document.

# 2  PHISHING RISK ASSESSMENT

100%

A single user clicking a phishing email can introduce significant risk to your business. Phishing attacks remain the highest risk to an organisation within current attack vector trends. A phishing email can lead to credential harvesting, data loss scenarios, ICO submission requirements, trojans and even ransomware. The templates used are real phishing attack content that have been used by attackers.
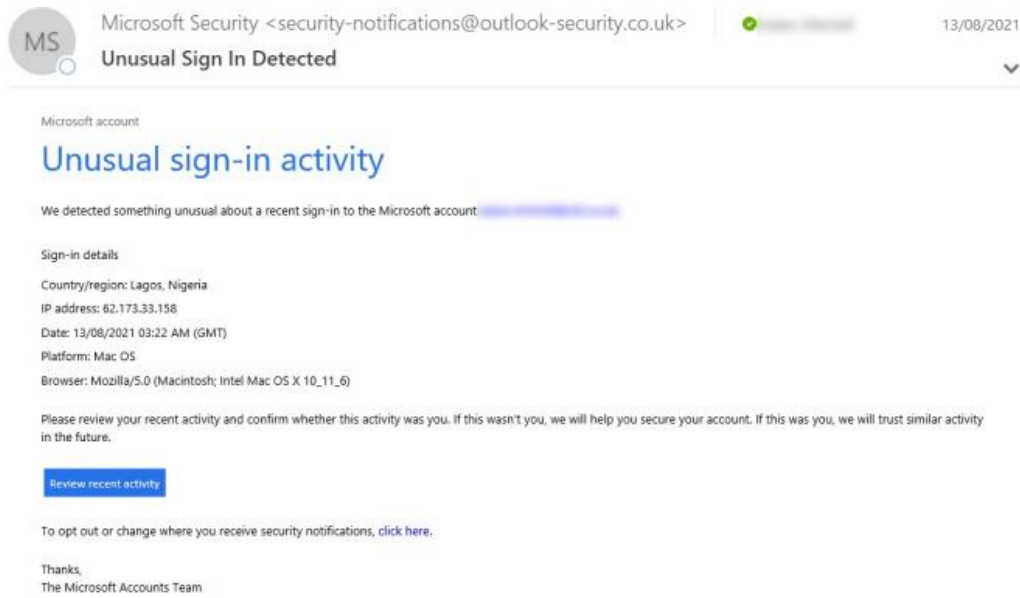
## 2.1  RESULTS

| Result | Count |
|---|---|
| Email Sent | 30 |
| Clicked Link | 0 |

Below are the first 10 results of the simulation:

| User email | Status | Result |
|---|---|---|
| User 1@test.com | Email Sent | Pass |
| User 2@test.com | Email Sent | Pass |
| User 3@test.com | Email Sent | Pass |
| User 4@test.com | Email Sent | Pass |
| User 5@test.com | Email Sent | Pass |
| User 6@test.com | Email Sent | Pass |
| User 7@test.com | Email Opened | Pass |
| User 8@test.com | Email Sent | Pass |
| User 9@test.com | Email Sent | Pass |
| User 10@test.com | Email Sent | Pass |

Detailed results of the phishing assessment have been provided in the Cyber Security Risk Assessment annex document.

## 2.2 DESIGN

The following template design was used for this phishing campaign:



MS  Microsoft Security <security-notifications@outlook-security.co.uk>  ●  ▓▓▓▓▓▓  13/08/2021

**Unusual Sign In Detected**  ⌄

Microsoft account

## Unusual sign-in activity

We detected something unusual about a recent sign-in to the Microsoft account ▓▓▓▓▓▓▓▓▓▓▓▓

Sign-in details

Country/region: Lagos, Nigeria

IP address: 62.173.33.158

Date: 13/08/2021 03:22 AM (GMT)

Platform: Mac OS

Browser: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)

Please review your recent activity and confirm whether this activity was you. If this wasn't you, we will help you secure your account. If this was you, we will trust similar activity in the future.

[ Review recent activity ]

To opt out or change where you receive security notifications, click here.

Thanks,
The Microsoft Accounts Team

# 3  MAIL FLOW PROTECTION

35%

This section has been added as Solace Cyber believe that enhancing your mail flow protections can significantly reduce the risks of malicious emails arriving at your staff. This section reviews the position around SPF, DKIM and DMARC.

| Domain | SPF | DKIM | DMARC | Score |
|--------|-----|------|-------|-------|
| Domain 1 | On | On | On | 50% |
| Domain 2 | On | On | On | 50% |
| Domain 3 | On | Off | Off | 25% |
| Domain 4 | On | Off | Off | 25% |
| Domain 5 | On | Off | Off | 25% |
| Domain 6 | On | On | On | 100% |
| Domain 7 | On | Off | Off | 25% |
| Domain 8 | Off | Off | Off | 0% |
| Domain 9 | On | Off | Off | 25% |
| Domain 10 | On | Off | Off | 25% |

# 4  MICROSOFT 365 SECURITY ASSESSMENT

<div style="background:#2196d3;color:#fff">18%</div>

Solace Cyber observe that a high percentage of Microsoft 365 customers are configured with default configurations. Cyber attackers are aware of this and will take advantage of the gaps. With a high percentage of cyber-attacks originating via phishing emails and other email attack vectors it is essential that Microsoft 365 is configured to optimal security configuration in conjunction with your business needs. The first step to protecting your email estate is to first understand where all the gaps are and what can be done to resolve these gaps.

Solace Cyber's Microsoft 365 Health Check reviews your Microsoft 365 configuration and provides a summary and score of your security posture. Detailed recommendations can be provided on how to security harden the Microsoft 365 tenant. The cost of an email breach can be as high as £100,000 due to the ICO and GDPR requirements that can arise from the sensitive and personal data that often exists within employee and company emails.

Microsoft's assessment of your security posture. Some insurers use Microsoft Secure Score to provide posture-based rates.

## 4.1  RECOMMENDED HEALTH CHECK ACTIONS

| Improvement Action | Category |
|---|---|
| Require MFA for administrative roles | Identity |
| Ensure all users can complete multi-factor authentication for secure access | Identity |
| Enable policy to block legacy authentication | Identity |
| Do not expire passwords | Identity |
| Turn on user risk policy | Identity |
| Turn on sign-in risk policy | Identity |
| Do not allow users to grant consent to unmanaged applications | Identity |
| Turn on customer lockbox feature | Apps |
| Restrict anonymous users from joining meetings | Apps |
| Only invited users should be automatically admitted to Teams meetings | Apps |
| Configure which users are allowed to present in Teams meetings | Apps |

# 5  USER MFA ASSESSMENT

<div style="background:#2e9bd6;color:white;">35%</div>

Credential harvesting is one of the most lucrative areas for cyber attackers. Millions of records are published daily across the dark web and sold between attacking groups. The growth is so large that criminal organisation will solely focus upon credentials harvesting and selling that data to other attack groups to utilise it. Without MFA all the attackers require is a username and password and they can access your users email content. If that content has personal data that can lead to costly ICO recoveries. Our CSIRT team is also seeing email content being edited leading to financial fraud, outbound spam spreading the compromise to other users and your clients and malicious payloads being dropped into the estate via the same entry methods. With MFA in place the attackers also must have access to the user's personal devices or unique codes to access the account.

MFA is a simple, cost-effective strategy that can be highly effective at deterring and preventing email attacks.

## 5.1  USERS

17 of 67 standard users have MFA enabled, giving a score of 25%.

| Criteria | Count |
|---|---|
| MFA Disabled | 50 |
| MFA Enabled | 17 |

## 5.2  ADMINISTRATORS

5 of 13 users with administrative permissions have MFA enabled, giving a score of 0%. This is due to the implied risks of an unsecured administrative account.

| Criteria | Count |
|---|---|
| MFA Disabled | 8 |
| MFA Enabled | 5 |

# 6  MICROSOFT 365 FORENSIC AUDIT

0%

There was clear evidence found of malicious forwarding rules and logins from non-UK locations from known malicious IP's. This user was not using a VPN and due to Covid-19 these logins were impossible. This same user had malicious forwarding rules created just after the first Belgium logins where emails are being sent to the RSS Subscriptions folder hiding them from the user.

User: Joe.Bloggs@domain.com is compromised

| UserLoggedIn | 2020-07-22T08:51:35 | Mozilla/5.0 (Windows NT 10.0; V | 198.97.15.19 | Palantir Technologies Inc. | London | England | United Kingdom |
|---|---|---|---|---|---|---|---|
| UserLoggedIn | 2020-07-22T08:51:35 | Mozilla/5.0 (Windows NT 10.0; V | 198.97.15.19 | Palantir Technologies Inc. | London | England | United Kingdom |
| UserLoggedIn | 2020-07-22T08:51:40 | Mozilla/5.0 (Windows NT 10.0; V | 198.97.15.19 | Palantir Technologies Inc. | London | England | United Kingdom |
| UserLoggedIn | 2020-07-22T08:51:42 | Mozilla/5.0 (Windows NT 10.0; V | 198.97.15.19 | Palantir Technologies Inc. | London | England | United Kingdom |
| UserLoggedIn | 2020-07-27T07:55:43 | Mozilla/5.0 (Macintosh; Intel Ma | 85.201.200.28 | Brutele SC | Mons | Wallonia | Belgium |
| UserLoggedIn | 2020-07-27T08:02:34 | Mozilla/5.0 (Macintosh; Intel Ma | 85.201.200.28 | Brutele SC | Mons | Wallonia | Belgium |
| UserLoggedIn | 2020-07-27T08:02:43 | Mozilla/5.0 (Macintosh; Intel Ma | 85.201.200.28 | Brutele SC | Mons | Wallonia | Belgium |
| UserLoggedIn | 2020-07-27T08:02:43 | Mozilla/5.0 (Macintosh; Intel Ma | 85.201.200.28 | Brutele SC | Mons | Wallonia | Belgium |
| UserLoggedIn | 2020-07-27T08:02:46 | Mozilla/5.0 (Macintosh; Intel Ma | 85.201.200.28 | Brutele SC | Mons | Wallonia | Belgium |
| UserLoggedIn | 2020-07-27T08:02:46 | Mozilla/5.0 (Macintosh; Intel Ma | 85.201.200.28 | Brutele SC | Mons | Wallonia | Belgium |
| UserLoggedIn | 2020-07-27T08:02:47 | Mozilla/5.0 (Macintosh; Intel Ma | 85.201.200.28 | Brutele SC | Mons | Wallonia | Belgium |
| UserLoggedIn | 2020-07-27T08:02:48 | Mozilla/5.0 (Macintosh; Intel Ma | 85.201.200.28 | Brutele SC | Mons | Wallonia | Belgium |
| UserLoggedIn | 2020-07-28T11:15:30 | Mozilla/5.0 (Windows NT 10.0; V | 198.97.14.67 | Palantir Technologies Inc. | New York | New York | United States |
| UserLoggedIn | 2020-07-28T11:15:39 | Mozilla/5.0 (Windows NT 10.0; V | 198.97.14.67 | Palantir Technologies Inc. | New York | New York | United States |
| UserLoggedIn | 2020-07-28T11:15:40 | Mozilla/5.0 (Windows NT 10.0; V | 198.97.14.67 | Palantir Technologies Inc. | New York | New York | United States |
| UserLoggedIn | 2020-07-28T11:15:40 | Mozilla/5.0 (Windows NT 10.0; V | 198.97.14.67 | Palantir Technologies Inc. | New York | New York | United States |
| UserLoggedIn | 2020-07-28T11:15:42 | Mozilla/5.0 (Windows NT 10.0; V | 198.97.14.67 | Palantir Technologies Inc. | New York | New York | United States |
| UserLoggedIn | 2020-07-28T11:15:43 | Mozilla/5.0 (Windows NT 10.0; V | 198.97.14.67 | Palantir Technologies Inc. | New York | New York | United States |

## Finding

A review of the Microsoft Admin Portal shows that all legacy authentication protocols are allowed.

Outlook Client, Exchange ActiveSync (EAS), Autodiscover, IMAP4, POP3, Authenticated SMTP, Exchange Online PowerShell

Whilst there is a rule for blocking legacy authentication protocol methods, it is configured in report-only mode and is not enabled.

## Recommendation

The Solace Cyber CSIRT team has seen high numbers of breaches entering via legacy authentication methods such as IMAP, POP3 and SMTP.

The current configuration is a significant security risk and needs to be addressed.

## Supporting Evidence



Multiple other users have been referenced on https://haveibeenpwned.com/.

# 7 BACKUP & DISASTER RECOVERY REVIEW

## 25%

The backup and DR solution for virtual machines is XXX. This product sits on a Synology NAS that also provides the backup storage natively. The application servers are somewhat static, so the recovery points required are not urgent. Office 365 & SharePoint is where company data is stored. This is natively resilient within Office 365 but also backed up with a Synology NAS using inbuilt Office 365 backup software.

| Criteria | Status |
|---|---|
| Backup | False |
| Offsite Backup | False |
| Air Gapped Backup | False |
| Immutable LTR Backups | False |
| DR Plan in place | False |
| DR Plan is documented | False |
| RPO and RTO requirements understood and met | False |
| Regular backup testing | False |
| Regular DR testing | False |
| Backup & DR monitored daily | False |

The backup strategy is considered adequate for the servers and services in operation however offsite and air-gapped backups are a must to ensure safeguards against DC failure or malware that could encrypt servers, VMFS data stores and the Synology backup device. All these devices have had historically documented vulnerabilities that ended up compromised and encrypted. Additionally, offsite DR services should be considered to allow customer services to be restored quickly and active/active services to be enabled where possible. Running active/active and air-gapped backup is still recommended.

| Criteria | Summary |
|---|---|
| Backup Solution | XXX, Synology NAS |
| Backup Storage Location | XXX, Synology NAS |
| Disaster Recovery Solution | None |
| Disaster Recovery Storage Location | None |
| Company Data Storage Location | None |

# 8 REMOTE WORKER SECURITY REVIEW

Remote working is now standard practice for many businesses since employees were forced home due to the 2020 pandemic, as the benefits of increased flexibility were realised more widely. The security implications of this largely forced operational decision present some challenges.

## 8.1.1 END USER SECURITY OVERVIEW

Customer X currently use Trend Worry Free Anti-Virus. This offers traditional antivirus features along with some additional behaviour-based malware detection to in the fight against ransomware. Although it does provide several requirements for modern endpoint protection it does not offer full visibility into attack forensics, automated roll-back, stop lateral movement or automated controls to eliminate unpatched vulnerabilities.

| Feature | Trend Worry Free | EDR |
|---|---|---|
| Stops lateral movement | No | Yes |
| Stops data exfiltration | No | Yes |
| Stores security forensics for root cause determination | No | Yes |
| Behavioural based detection | Yes | Yes |
| Includes signature-based pattern detection | Yes | No |
| Machine Learning | Yes | Yes |
| Deny access to files systems to prevent ransomware encryption and registry tampering | No | Yes |
| Stop the breach in real-time | No | Yes |
| Stops Command and Control | No | Yes |
| SOC service provided with 24/7/365 cover | No | Yes |
| Orchestrated incident response | No | Yes |

| Criteria | Status |
|---|---|
| Centrally Managed Remote Access Policies | Yes |
| MFA required for remote access | No |
| Single Identity (SSO) enabled for all web apps and remote access | No |
| Remote access audit logging | No |
| Remote worker web access filtering | No |
| Anti-malware comprehensive coverage, centrally managed and maintained | Yes |
| Endpoint device vulnerability management, at least monthly | No |
| Have you implemented application whitelisting | Yes |
| Controls in place for local administrator privileges of end user devices | Yes |
| Do you control network and data access using a zero-trust access model | No |

# 9  FIREWALL REVIEW

40%

Customer X currently use Trend Worry Free Anti-Virus. This offers traditional antivirus features along with some additional behaviour-based malware detection to in the fight against ransomware. Although it does provide several requirements for modern endpoint protection it does not offer full visibility into attack forensics, automated roll-back, stop lateral movement or automated controls to eliminate unpatched vulnerabilities.

Firewalls have often been seen as a drop-in solution to secure a network and vendors have made huge progress trying to make that a reality. As firewalls have become more complicated and feature rich the potential for misconfiguration has increased and Solace Cyber often see firewalls with features that are not configured at all. They also need to be considered in the context of your wider strategy around remote working, public facing services and consumption of Cloud applications.

| Finding | Suggestion |
|---|---|
| HA is not working at Poole | Reboot and firmware upgrade |
| Firmware is out of date on both devices | Upgrade firmware at frequent intervals |
| Remote access does not have multi-factor authentication enabled | Enable multi-factor authentication |
| IPS is enabled but does not perform SSL inspection | Configure IPS with SSL inspection |
| Publicly accessible services are on the LAN network zone | Move publicly accessible services into DMZ network zone |
| HA pair failure has not alerted | Investigate reason for HA failure and failure to alert |

# 10 CYBER INSURANCE ASSESSMENT

<div style="background:#3399cc; color:white">47%</div>

Cyber insurance companies have come under huge strain in 2021 with the massive increase in cyber-attacks since Covid-19. With this additional cost it has become more apparent in cyber incident response processes that the insurance companies are being represented by organisations and individuals whose primary objective is to find evidence that the policy holder has not fulfilled their T&Cs within their insurance, thus voiding the cover. This article aims to increase awareness of the typical T&Cs added to insurance policies and to provide guidance and advice on how to ensure your company is remaining compliant.

Many cyber insurance policies - despite not having EDR as a requirement - will offer increased policy coverage if the business is protected with an EDR solution. IE £1m coverage without having EDR deployed, or £5m coverage with EDR deployed, for the same policy price.

No insurance policies have been provided. We have run an assessment against generic questions asked by a sample of key cyber insurance providers.

| Criteria | Status |
| --- | --- |
| Do you have a dedicated individual responsible for Information Security and Privacy? | Yes |
| Do you have a written incident management response plan? | No |
| Do you perform background checks on all employees and contractors with access to sensitive data? | No |
| Do you have written information security policies and procedures that are reviewed annually and communicated to all employees including information security awareness training? | Yes |
| Do you ensure all remote access to IT systems is secure? | Yes |
| Are annual or more frequent internal/external audit reviews (including penetration testing) performed on your IT network and your procedures? | No |
| Do you use anti-virus, anti-spyware and anti-malware software and update them regularly? | Yes |
| Do you use firewalls and other security appliances between the Internet and sensitive data? | Yes |
| Do you use intrusion detection or intrusion prevention systems (IDS/IPS) and are these monitored? | No |
| Do you ensure all sensitive data on your system is encrypted? | No |
| Do you ensure all sensitive data on all removable media is encrypted? | No |
| Do you perform regular backups and periodically monitor the quality of the backups? | No |
| Do you have a Disaster Recovery Plan (DRP)? | Yes |
| Do you have a Business Continuity Plan (BCP) in place? | Yes |
| Do you ensure all of your systems are not end-of-life? | No |
| Are your firewalls up to date with security patching? | No |

| Is security patching up to date so that there are no critical or high vulnerabilities outstanding? | No |