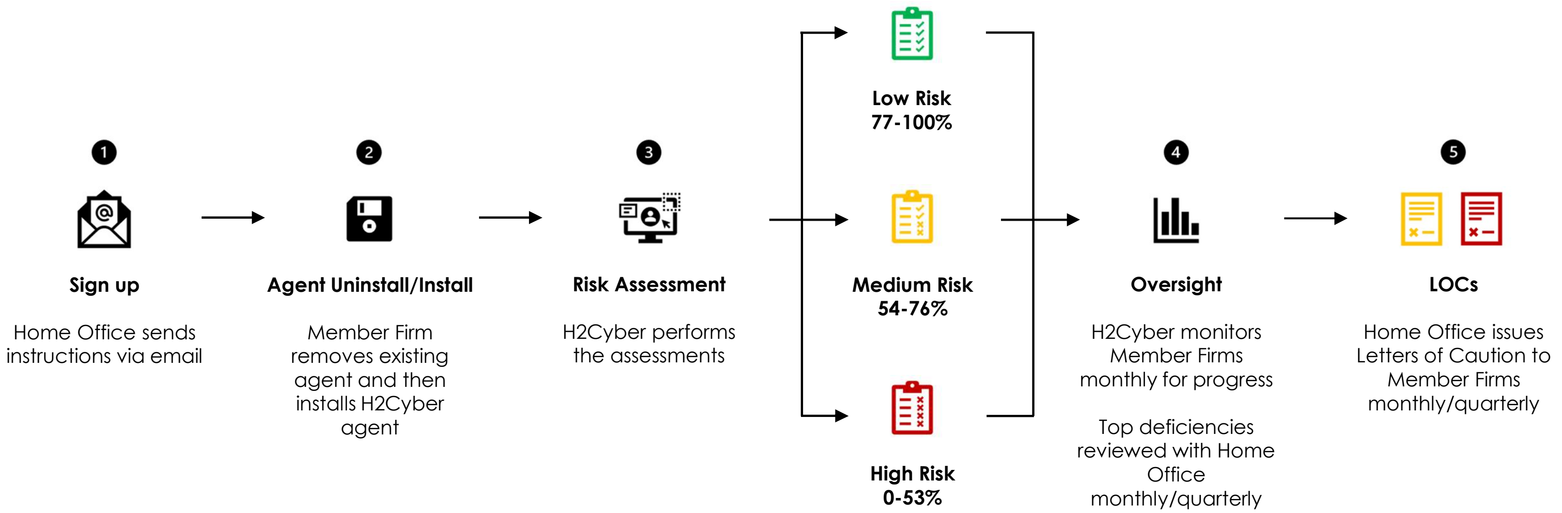
Broker Dealer - Oversight of Member Firms



1 **Sign up**

Home Office sends instructions via email

2 **Agent Uninstall/Install**

Member Firm removes existing agent and then installs H2Cyber agent

3 **Risk Assessment**

H2Cyber performs the assessments

Low Risk
77-100%

Medium Risk
54-76%

High Risk
0-53%

4 **Oversight**

H2Cyber monitors Member Firms monthly for progress

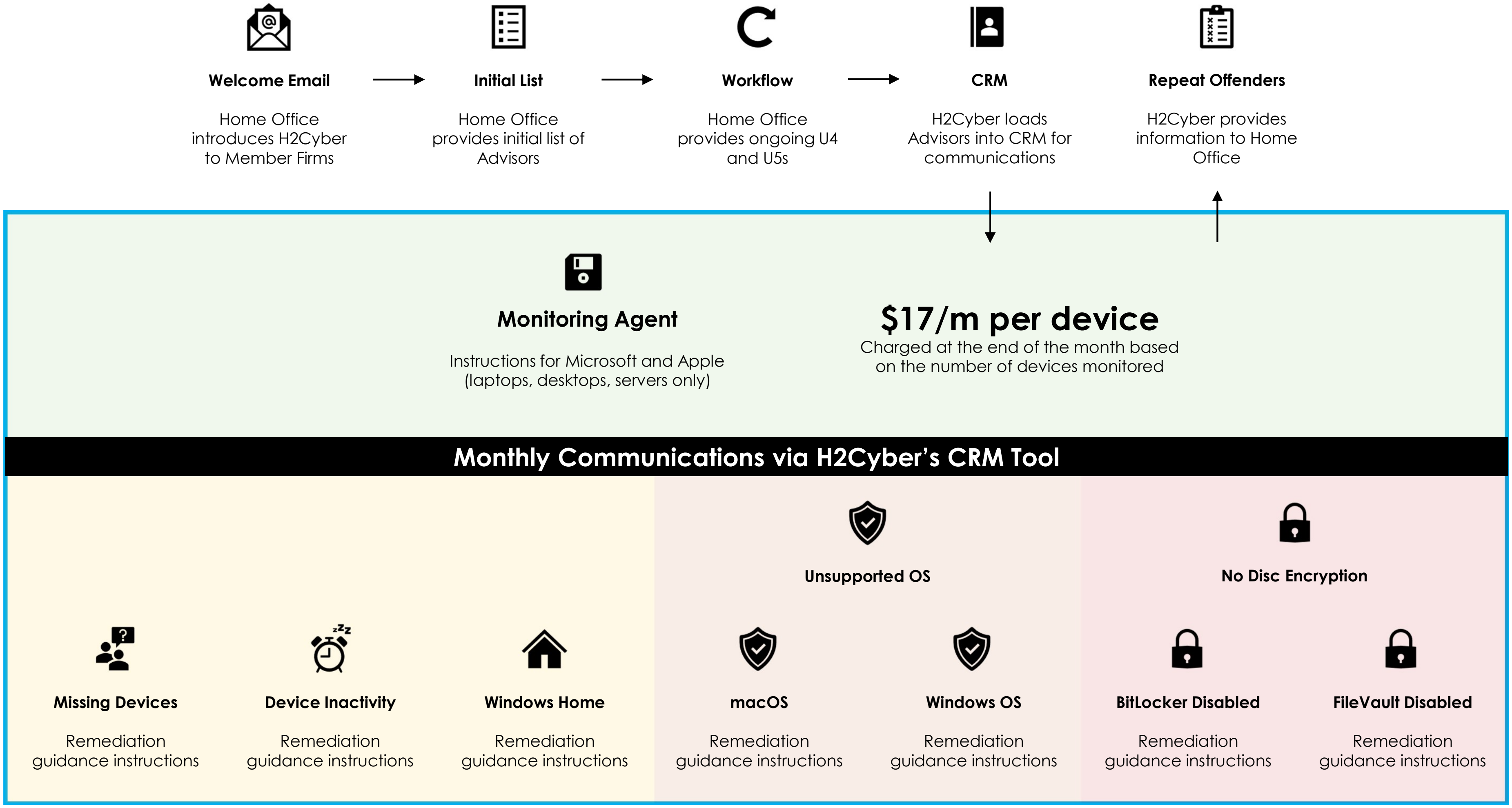
Top deficiencies reviewed with Home Office monthly/quarterly

5 **LOCs**

Home Office issues Letters of Caution to Member Firms monthly/quarterly

2022 Report on FINRA's Examination and Risk Monitoring Program

- Inadequate Risk Assessment Process
    - Not having an adequate and ongoing process to assess cyber and IT risks
- Branch Policies, Controls and Inspections
    - Not maintaining inventories of branch level software and hardware, inspections and automated monitoring programs



Welcome Email

Home Office introduces H2Cyber to Member Firms

Initial List

Home Office provides initial list of Advisors

Workflow

Home Office provides ongoing U4 and U5s

CRM

H2Cyber loads Advisors into CRM for communications

Repeat Offenders

H2Cyber provides information to Home Office

Monitoring Agent

Instructions for Microsoft and Apple (laptops, desktops, servers only)

$17/m per device

Charged at the end of the month based on the number of devices monitored

Monthly Communications via H2Cyber's CRM Tool

Unsupported OS

No Disc Encryption

Missing Devices

Remediation guidance instructions

Device Inactivity

Remediation guidance instructions

Windows Home

Remediation guidance instructions

macOS

Remediation guidance instructions

Windows OS

Remediation guidance instructions

BitLocker Disabled

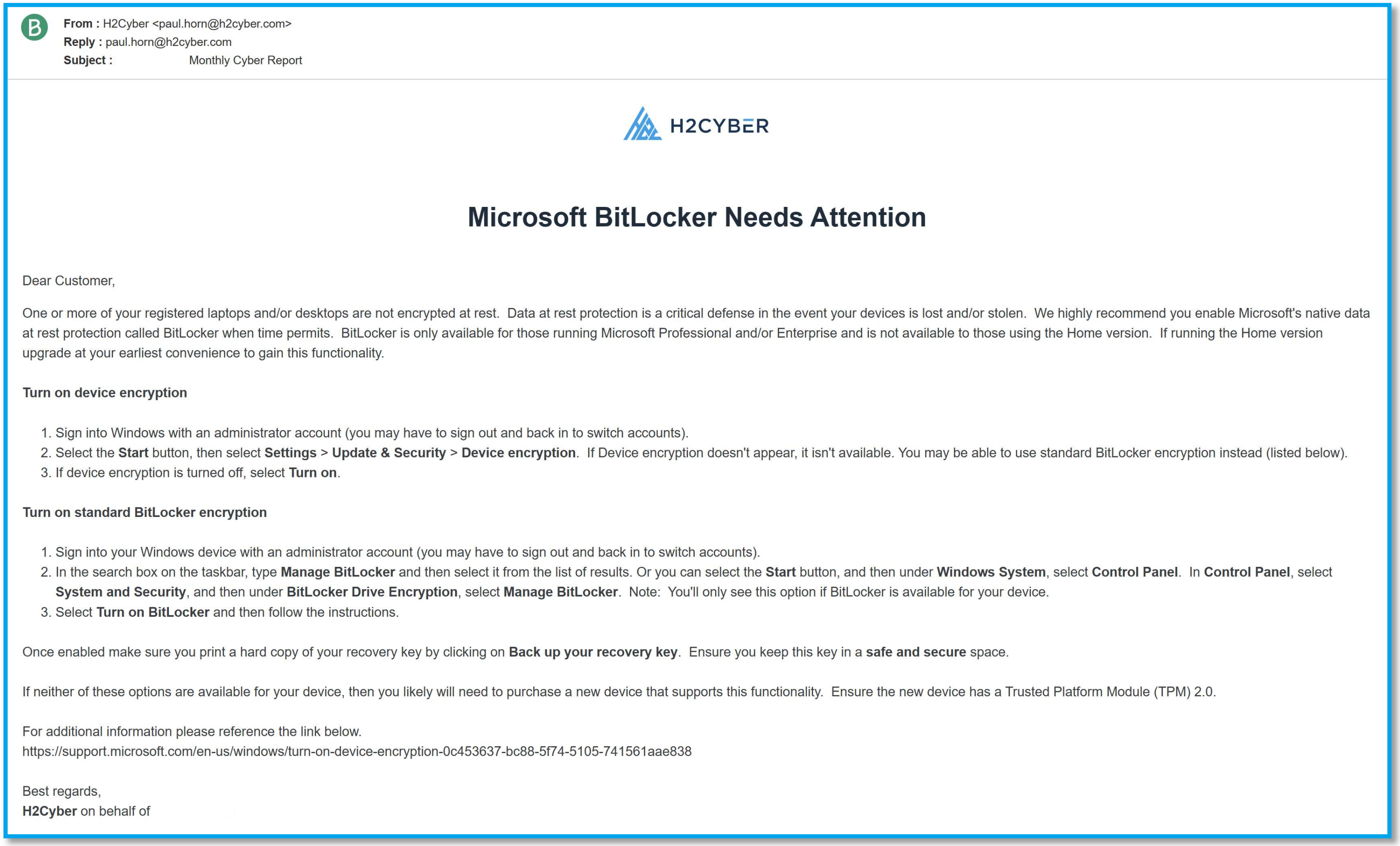
Remediation guidance instructions

FileVault Disabled

Remediation guidance instructions

Why is Antivirus not monitored?

Antivirus (free) is native to both Windows 10/11 (via Microsoft Defender) and macOS (via XProtect).
Neither allow for uninstallation only silence, when another antivirus is present.



From : H2Cyber <paul.horn@h2cyber.com>
Reply : paul.horn@h2cyber.com
Subject : Monthly Cyber Report

Microsoft BitLocker Needs Attention

Dear Customer,

One or more of your registered laptops and/or desktops are not encrypted at rest. Data at rest protection is a critical defense in the event your devices is lost and/or stolen. We highly recommend you enable Microsoft's native data at rest protection called BitLocker when time permits. BitLocker is only available for those running Microsoft Professional and/or Enterprise and is not available to those using the Home version. If running the Home version upgrade at your earliest convenience to gain this functionality.

Turn on device encryption

1. Sign into Windows with an administrator account (you may have to sign out and back in to switch accounts).
2. Select the **Start** button, then select **Settings** > **Update & Security** > **Device encryption**. If Device encryption doesn't appear, it isn't available. You may be able to use standard BitLocker encryption instead (listed below).
3. If device encryption is turned off, select **Turn on**.

Turn on standard BitLocker encryption

1. Sign into your Windows device with an administrator account (you may have to sign out and back in to switch accounts).
2. In the search box on the taskbar, type **Manage BitLocker** and then select it from the list of results. Or you can select the **Start** button, and then under **Windows System**, select **Control Panel**. In **Control Panel**, select **System and Security**, and then under **BitLocker Drive Encryption**, select **Manage BitLocker**. Note: You'll only see this option if BitLocker is available for your device.
3. Select **Turn on BitLocker** and then follow the instructions.

Once enabled make sure you print a hard copy of your recovery key by clicking on **Back up your recovery key**. Ensure you keep this key in a **safe and secure** space.

If neither of these options are available for your device, then you likely will need to purchase a new device that supports this functionality. Ensure the new device has a Trusted Platform Module (TPM) 2.0.

For additional information please reference the link below.
https://support.microsoft.com/en-us/windows/turn-on-device-encryption-0c453637-bc88-5f74-5105-741561aae838

Best regards,
H2Cyber on behalf of