Cybersecurity Posture Assessment Report

ATTAINABLE SECURITY

Cybersecurity Assessment
and
Prioritized Action Plan
Prepared for:

DUNDER MIFFLIN, INC.
PAPER COMPANY

ATTAINABLE SECURITY

Table of Contents

ATTAINABLE SECURITY

Summary

We are excited to provide your finalized cybersecurity assessment report. We have broken down this report into sections for each domain that we assessed.

In our assessment, we reviewed Dunder Mifflin by evaluating an internally developed list of seven domains. This list of domains was inspired by the following NIST publications:

- NIST Special Publication 800-53Ar5
- NIST Special Publication 800-53B
- NIST Cybersecurity Framework (CSF) 2.0

In summary, Dunder Mifflin has several fundamental security practices already in place as a result of the security defaults enforced by their Microsoft 365 tenant, such as MFA, account lockout thresholds, etc.

Dunder Mifflin is in a strong position to improve their security posture in several domains. Specifically, the most significant improvements can be made to their endpoint protection, data protection, access controls, and employee training and awareness. These improvements will help bring Dunder Mifflin in line with best cybersecurity practices.

ATTAINABLE SECURITY

Access Controls

We reviewed your current access controls, including:

- Adherence to the Principle of Least Privileged Access
- Adherence to Role-Based Access Controls (RBAC)
- Current implementation of account management and access cutoff processes

Current State

Dunder Mifflin is currently not following the principle of least privileged access, with owner and admin level access being granted to users that are not supposed to have that level of access.

For example, several global administrators were detected in their Microsoft 365 tenant, and multiple department-specific SharePoint sites had edit-level access available to the entire organization.

Dunder Mifflin currently does not have an automated or consistent onboarding and offboarding process, leading to inconsistent permissions being granted upon onboarding, and the risk of access remaining post-offboarding.

Dunder Mifflin is currently not utilizing any role-based access controls (RBAC) to gate access to internal SharePoint sites or other resources. RBAC can help control additional resources once other third party apps are integrated via SSO/SCIM.

Recommendations

- Implement RBAC where appropriate.
- Restrict admin and owner level permissions to appropriate individuals.
- Implement an onboarding and offboarding checklist to ensure access is consistently granted and revoked.
- Conduct a full internal review of all access for third party apps, including Zoom, Slack, and Jira, to identify other potentially overprivileged accounts.

ATTAINABLE SECURITY

Authentication Methods

We reviewed your current authentication methods, including:

- MFA implementation and configuration
- Password requirements, such as strength, length, and complexity
- Password reset and recovery policy
- Account lockout policies
- Conditional access policies

Current State

Dunder Mifflin has been leveraging their Microsoft 365 Entra ID tools to great effect. They have adhered to the security defaults, allowing them to take advantage of features like MFA for both their standard and administrator accounts.

There are opportunities to leverage advanced Entra ID authentication methods, such as conditional access policies, and to extend these access controls to other cloud applications in use by Dunder Mifflin by way of SSO/SCIM integration.

The use of SMS and voice-based 2fa methods is currently enabled, which puts the organization at risk of low-difficulty sim swap attacks.

Recommendations

- Implement SSO and/or SCIM for Dunder Mifflin's other core applications, allowing them to benefit from security features in Entra:
    - Zoom
    - Slack
    - Jira
- Restrict MFA authentication options exclusively to phishing-resistant methods, disabling SMS and voice-based options.
    - While there are several powerful phishing resistant options in the market like Yubikeys, the Microsoft Authenticator app supports a simplified phishing-resistant option that is more secure than traditional prompt-based MFA options.

- Standardize around a single authenticator app for a consistent user experience, and so that documentation may be developed around that tool.
    - As Dunder Mifflin is a Microsoft 365 tenant, the Microsoft Authenticator app is probably best.

Network Security

We reviewed your current network security and tooling, including:

- Physical network layout
- Network segmentation configuration
- Configured network threat hunting tools
- VPN and remote access configuration
- Wireless network security settings

Current State

Dunder Mifflin current network infrastructure is as sophisticated as it needs to be: no on-premesis infrastructure exists in its single office, other than whatever endpoints are onsite when users work from the office, and a few problematic printers.

With that said, clients do come into Dunder Mifflin's office from time to time, and it is worth configuring a dedicated guest network that clients and other external users can use. This would minimize the risk that unknown devices pose to their internal network.

The large number of remote workers that Dunder Mifflin maintains enforces the need to move towards a zero-trust security model.

Given that Dunder Mifflin currently has no security measures in place to protect or encrypt network traffic from its endpoints, a simple VPN solution like Cloudflare WARP would ensure that all traffic from all endpoints would be encrypted, regardless of location, network, or application being used.

Recommendations

- Implement Cloudflare WARP for all endpoints, ensuring that all traffic is encrypted.
- Replace the copier machine, or the desk chairs. The manager will have to make the call.
- Configure a dedicated guest network for the office

    - Enable client device isolation on the guest network to prevent guest devices from seeing/communicating with each other when connected
- Develop policies and documentation around remaining secure when working remotely

ATTAINABLE SECURITY

Endpoint Protection

We reviewed your current endpoint protection solution, including:

- Antivirus and Anti-malware configuration
- Attack surface reduction settings
- Configuration policies
- Patch management solution

Current State

Dunder Mifflin currently relies on the built-in security provided by Windows Defender, without any additional systems in place. This leaves their endpoints vulnerable to all sorts of attacks, and leaves the organization without the visibility and information it needs to protect its infrastructure.

There is also a lack of documentation including policies and procedures for how Endpoints should be protected. The development of an incident response plan and several basic incident response playbooks is critical.

There is no mobile device management (MDM) or remote monitoring and management (RMM) tooling currently in place, leading to little visibility. This also means that Dunder Mifflin is not able to properly monitor, manage, or enforce any kind of policies onto their endpoints.

Recommendations

- Implement a Managed Detection and Response (MDR) platform
    - With their current E3 licenses, the most cost effective solution would be Microsoft Defender for Endpoint
- Implement an MDM solution
    - With their current E3 licenses, the most cost effective solution would be Microsoft Intune
- Implement an RMM solution
- Develop configuration policies that will help secure endpoints further

ATTAINABLE SECURITY

Employee Training and Awareness

We reviewed your current security and awareness training program, including:

- Assigned training materials
- Training schedule
- Mock phishing campaign schedule
- Internal policy awareness and accessibility
- Integration with new hire on-boarding
- Regulatory compliance of training program

Current State

Dunder Mifflin does not currently utilize any formal security and awareness training, leaving the preparedness of its workforce up whatever technical and security awareness each individual team member happens to already possess.

With over 90% of breaches involving human error, the training of an organization's workforce is of paramount importance. Additionally, Dunder Mifflin does not have any standing policy documents that speak to the organization's expectations in this area.

There are solutions that provide both security awareness training and mock phishing campaign services. These are often referred to as "Human Risk Management" platforms.

Recommendations

- Invest in a security awareness training platform to train up the workforce
- Invest in a mock phishing campaign platform to help train the workforce to recognize and report phishing emails
- Develop policy documents around acceptable use of technological resources, and around best practices, including:
    - Secure remote working standard
    - Acceptable use policy
    - How to report suspicious emails

ATTAINABLE SECURITY

Data Protection

We analyzed your current data protection implementation, including:

- Data encryption settings
- Backup and recovery configuration

Current State

Dunder Mifflin currently has no formalized backup systems in place. Given that they utilize SharePoint and OneDrive to store internal data, there is limited backup and restore functionality in place, but it does not satisfy the requirements that a fully-fledged backup solution would provide.

Any data that is stored on endpoints that is not being uploaded to OneDrive or SharePoint is currently completely unprotected, even by the basic resiliency offered by OneDive and SharePoint.

Additionally, data stored on endpoints is further at risk because disk-level encryption is not enforced.

Recommendations

- Implement a 3-2-1 backup system
    - Three backups total
    - Two different backup formats
    - One offsite backup
- Enforce disk-level encryption on all endpoints
- Explore ransomware-rollback products

ATTAINABLE SECURITY

Shadow IT

We reviewed any evidence of Shadow IT in your organization, including:

- Inventory of authorized applications and services
- Inventory of unauthorized applications and services
- Potential security vulnerabilities resulting from use of unauthorized applications and services

Current State

Dunder Mifflin has basic visibility into some third party apps used by its workforce, with the visibility provided by basic Entra and Cloud App Security features. However, there are no systems in place that can help control Shadow IT activity, and the organization does not have a formal stance on Shadow IT activity.

Having a formal stance and building out pathways to accept or reject potential apps can help significantly control the use of Shadow IT.

Recommendations

- Build out policies to formally approve or reject apps for use within the organization
- Establish a repository of formally approved apps, and an easy way for users to request access to those apps
    - SSO and SCIM integrations are potentially available for these apps
- Configure alerting for potentially unsafe, inappropriate, or illegal activity.
    - This should be configured to reflect whatever the organization defines within their acceptable use policy

Prioritized Action Plan

ATTAINABLE SECURITY

Prioritized Action Plan

The plan below is a list of tailored, prioritized items for your business to take action on in order to improve its security posture.

Recommendation	Implementation Complexity	Financial Cost	Time Cost	Criticality
Implement a Human Risk Management solution	**Medium** Some HRM solutions are relatively turn-key, but customization must still be done to reflect the org's priorities	**Low** HRM solutions range from 2-5 dollars per month, per user.	**Medium** Launching the HRM solution takes several weeks to fine tune and set up curriculums and campaigns, but it can be relatively low maintenance afterwards	Critical
Implement an RMM solution	**High** Requires accessing devices manually and/or local users executing commands. Can be automated if an MDM is installed first.	**Medium** RMM tooling costs around $5 per endpoint per month.	**Medium** Most of the time cost will revolve around adjusting user expectations, as the agents can be deployed quickly.	Critical

ATTAINABLE SECURITY

Recommendation	Implementation Complexity	Financial Cost	Time Cost	Criticality
Implement an MDM solution	**High** Most of the implementation complexity revolves around developing device and compliance policies, as well as orgwide settings	**Medium** MDM solutions can cost up to $20 per endpoint per month.	**Medium** Requires accessing devices manually and/or local users executing commands. Can be automated if an RMM is installed first.	Critical
Implement an MDR solution	**Medium** MDR solutions can be deployed via RMM and/or MDM solutions.	**Low** MDR solutions can cost between $5 and $20 per endpoint per month. Many organizations will offer MDR as part of a larger package, like Microsoft's Defender	**Medium** Calibration will be required for the MDR to operate properly, but that happens naturally over time.	Critical
Implement a 3-2-1 backup solution	**Low** Backup solutions are relatively simple to implement, with many turn-key solutions available on the market.	**Medium** Backup solutions scale in cost as the amount of data covered and number of backup destinations increase.	**Low** Initial backups can begin almost immediately upon purchasing licenses.	High

ATTAINABLE SECURITY

Recommendation	Implementation Complexity	Financial Cost	Time Cost	Criticality
Develop internal security policies	**High** Depending on the business processes that need to be documented, and the level of detail of each of the documents, creating the policies and processes to review and update them regularly can be fairly complex	**Low** Usually, these documents can be created in Microsoft Word or another program that is already included in the business tooling, and stored on existing business resources like Microsoft 365 or an on-premises file server.	**High** Creating the documents and ensuring that they properly cover the business use cases can take up a significant amount of time, and there will also be a recurring time commitment to review and update the documents regularly (e.g., at least annually).	High
Enforce encryption on all endpoints	**Low** Encryption can be configured by a simple flip-switch once an MDM is in place.	**N/A: Enforcing encryption is free**	**Low** Endpoints may be required to restart once encryption is enabled and enforced.	High
Deploy Cloudflare WARP	**Low** Cloudflare Warp requires minimal user training. The UI is a single toggle.	**N/A:** Cloudflare WARP is free	**Low** Cloudflare Warp can be pushed out in seconds via RMM or MDM.	Medium

ATTAINABLE SECURITY

Recommendation	Implementation Complexity	Financial Cost	Time Cost	Criticality
Restrict administrator privileges	**Medium** Restricting local administrator rights on employee endpoints will significantly reduce the attack surface of the organization and prevent certain pieces of malware from running altogether on the system. Depending on how the employee endpoints are configured, the complexity of this process can vary.	**Low** Requires no additional tooling once MDM and/or RMM solution is sourced.	**Medium** MDM tooling will allow you to create a policy that restricts local administrator privileges. RMM tooling will provide technical support staff with a way to remotely support employee devices when interacting with various administrative functions like User Access Control (UAC) prompts.	Medium
Conduct a full internal access review for third party apps	**Medium** Requires Dunder Mifflin to identify all approved applications and then discover all apps currently in use.	**Low** Can be free at the cost of time. Tools exist to make this process easier.	**High** The initial audit can be extremely time consuming, especially when there is no identified baseline.	Low