Data Privacy Assessment Project

Company background:

Agarwal, Becker, and Cooper (ABC) PC, a Certified Public Accounting firm, has been providing quality, personalized financial guidance to individuals and businesses for over 30 years. Their expertise ranges from tax management and accounting services to more in-depth services such as audits of financial statements, preparation of financial statements, consulting and financial planning. The main office is in Glendale, California with satellite offices in Seattle, Washington, and Aurora, Colorado. They have approximately 100 employees and 1000 clients in multiple US western states. Five of these clients are also co-located in Ireland, the Netherlands, and Germany. They have designated the Chief Accounting Officer (CAO) as their Data Protection Officer (DPO) and their IT support analyst as their Information Security Officer (ISO).

While they use a variety of financial applications for their business, they have requested a privacy assessment of their Microsoft 365 Business Premium service. This includes their use of Outlook, Excel, Word, OneDrive, SharePoint, and Teams, all of which may have PI. ABC PC uses the Microsoft 365 Azure Active Directory (Azure AD) for its cloud-based user identity and authentication service and Intune for Microsoft system and application updates. Note that ABC is initiating project to use Microsoft Power BI for data analytics of its customers. All employees use Windows 10 with a migration path to Windows 11.

Currently has two Microsoft Server 2019 servers on prem: 1 for Active Directory Domain Services (AD DS) and 1 for client file transfers. Client accounts are given a local AD DS user ID and password to upload / download financial files with their company reps. Two junior analysts monitor the file share and move the files to/from the financial services employee's personal SharePoint folder.
For employees, user account exists in AD DS and a copy is also in the Azure AD tenant for their Microsoft 365 subscription. Project in place to move this to Azure in the next 6 months.

Personnel

- 50 full-time tax / finance accountants
    - During tax season, this number is supplemented by approximately 25 contractors and temporary workers.
- 25 support personnel / management
    - 8 Internal Auditors
    - 2 IT personnel, 1 Manager and one systems/network/application administrator
    - 5 Leadership (CEO, CAO, CMO, COO, Executive VP)
    - 9 salespeople
    - 1 internal attorney with external support
- Employee location:
    - 20% in the office, 50% hybrid, 30% remote
    - All employees have remote work capabilities
- Data Protection Officer (DPO): Tracy Bingham
    - They also act as the Chief Accounting Officer who signs all contracts
- Information Security Officer (ISO): Thomas Brooks

    - They also act as the ABC IT Manager

Client locations:

- United States
    - California
    - Nevada
    - Oregon
    - Washington (state)
    - Arizona
    - Utah
    - Colorado
- Europe
    - Ireland
    - The Netherlands
    - Germany

Applicable Contracts:

- Microsoft 365 Business Premium (Signed April 1, 2021. Entered into service, July 1, 2021)
    - Power BI add-on (Signed December 1, 2021. Entered into service, March 1, 2022)
- Business Clients
    - Financial management
    - Tax services
- Individual Clients
    - Financial management
    - Tax services

Systems / Applications:

- Windows 10 laptops and desktops
- Microsoft 365 Business Premium (Cloud)
    - Microsoft 365 Azure Active Directory (Azure AD)
    - Email (Outlook & Exchange)
    - OneDrive / Sharepoint / Teams
    - Office applications (Word, Excel, PowerPoint)
- Data Analytics
    - Microsoft Power BI
- Website
    - Externally sourced and managed
    - Used for marketing purposes
- Financial Management Systems (Cloud)
    - Tax
    - Financial
- Sales Management System (Cloud)
    - Sales
    - Client leads

- Legacy human resources running on Windows Server 2019
    - MS SQL
- Hosted website
    - Company information
    - Contact information
    - Form for contacting clients
    - Blog with ability for users to sign up for email notifications

Data types in use:

- Employee information
    - Demographic information
    - Job history
    - Education history
    - Health plan information
    - Photographic facial image
    - Certificate / License number(s)
    - Background check information
- Client demographics (individual and organization):
    - First / Last names
    - Mailing Address(es)
    - Phone number(s)
    - Email address(es)
    - Birthdate
    - Dependents (individual)
    - Social Security Number(s) / Employer Identification Number(s)
    - Driver's license number
    - Passport number
    - Website(s)
- Client Financial data:
    - Accounts receivable / payable
    - Income sources
    - Expenses
    - Bank information (account number)
    - Tax information (State, Federal)
    - Payment information
        - ACH
        - Credit card
- Other data:
    - Voice recordings (from voice mail and recorded client conversations with internal staff)

ABC PC Policies:

- Information Security and Acceptable Use Policy (Published & Last Review: January 1, 2021)
  This policy follows the NIST Cybersecurity Framework. Employees are required to acknowledge it upon employment and as part of annual training.
  This policy covers the following elements:
    - End user acceptable use of ABC systems and data
    - Roles and responsibilities
    - Network and system protection requirements
    - Risk management policy
- Data Classification and Protection Policy (Implemented: January 1, 2018, Last updated June 30, 2020)
  This policy provides employees with the organization's data classification schema and requirements for the protection of restricted PII, PHI and CHD. It also contains requirements for responding to a data breach to include communicating with individuals impacted.
    - Appendix: Data Retention Schedules
      Note: These follow all applicable laws and regulations based on the data types.
- Website Privacy Policy – Published on the ABC website (Last updated September 30, 2020)

ABC PC Procedures (Published March 1, 2021):

- Employee onboarding and termination procedures
- Incident Response & Disaster Recovery procedure
- System and Data Destruction procedures
- Individual access to PI procedures
  For individual accounts, they may request access to their files and PII through their account manager

Assessment information:

- ABC PC initially signed a contract to use Microsoft Office 365 in June 2018. On April 1, 2021, Tracy Bingham, the ABC PC CAO signed an updated Microsoft Services Agreement contract to update the Microsoft services provided to Microsoft 365 Business Premium. It was chosen as the lowest-cost option while providing cloud-based functionality. This contact establishes the relationship between ABC PC and Microsoft regarding security and data protection.

- Individual PII may be collected as a part of contracted financial or tax services. ABC Privacy Policies and procedures for handling client sensitive data, including PII, is included with client contracts. Privacy information is distributed to clients on an annual basis. It is the responsibility of the client contracting official to notify any individuals associated with the contracting services of ABC's privacy policies and procedures.

- Wherever possible, ABC provides timely and effective notice to the public and/or to clients about activities that impact their privacy. For those occasions where ABC cannot provide notice at the time the information is collected (e.g., when the information is collected by another agency or another organization), ABC provides notice via its Website Privacy Policy.

- Data Sources:
    - ABC's clients provide PII as a course of normal business. This information is uploaded into our tax and financial applications as the authoritative source of the information. It may be duplicated into M365 applications for communications and analysis.
    - ABC PC staff and contractors upload and store data that has been created or obtained in connection with its business activities. This include PII listed above. User-created content may also include information in the user's profile, emails, calendar, and other information voluntarily stored within M365.
    - ABC PC may receive tax and financial records that may be stored within M365 file shares and data repositories from validated outside resources with the explicit permission of its clients.
    - The public's information is not collected directly by M365. However, information provided by and pertaining to members of the public may be stored in M365. These individuals may include potential clients with interest in the firms' services.

- Access to the Microsoft 365 (M365) product suite is restricted to authorized ABC employees, who must adhere to corporate policies outlined above. Access to the information stored within M365 is dependent on the particular business purpose and the access permissions granted to a specific user.
    - Business analysts, financial and tax accountants have access to their directly assigned client data. They often share client data between multiple analysts / accountants. This may be through shared files/folders on SharePoint, OneDrive, Teams and local drives.
    - System administrators may have access to system data and system audit logs in order to manage access roles, monitor system usage, perform system audits, and complete other necessary job functions.
    - Authorized ABC contractors have access to information in M365, when necessary.
      All ABC contractors are required to sign NDAs, complete security and privacy training prior to obtaining access to any ABC systems, and complete annual security and privacy training to maintain network access and access to those systems.
      Contractors who access M365 are subject to the same rules and policies as ABC staff. Contractors must also follow the reporting and other procedures in the ABC's Incident Response Plan.

- Individual opportunity or right to decline to provide their PI depends on how the information is collected. ABC does not use M365 to collect information, including PII, directly from the public. However, ABC staff and contractors use M365 in furtherance of the ABC's services. Information collected through other sources, which includes PII, is maintained in M365.
  For example, ABC staff may include individual client PII in an email (Outlook), a document (Word), or spreadsheet (Excel) as a part of standard business communications, analysis, and reporting. As a part of the contracting process, individuals are given notice and request their information is not included in such documents.
  Individuals also receive email notifications regarding the use of PII within email with the option of contacting the ABC DPO to opt-out

- Since the M365 data is unstructured and generally unmanaged, there are no formal procedures in place for confirming information accuracy.
  Due to the nature of the system and the anticipated broad use of these services across the enterprise, information that is stored in M365 generally will not be checked for accuracy, completeness, accuracy, completeness, or currency. It is the responsibility of the employee / user to ensure the completeness, accuracy and currency of data at the time it is created or used within M365 products.

- System administrators ensure user information is complete and accurate for access control through Active Directory (AD) authentication, but will not ensure that data created or entered by end users is complete, accurate, or current. AD is updated immediately when a user account is disabled or terminated. User contact information is removed once the user account is deleted. Within the organization, users have the ability to enter their own information and to ensure that it is current

- All ABC Windows endpoints (laptops and desktops) follow a standard configuration build and distributed by the IT Manager. It includes Bitlocker hard drive encryption and Windows Defender. All Windows endpoints require a valid user-id and password following the standard group policy for access. All remote access requires the use of Microsoft Authenticator

- According to the ABC Data Retention Policy and destruction procedures, information in the ABC M365 cloud instance is retained and destroyed in accordance with applicable ABC policies and procedures, as well as with the published ABC records disposition schedule. PI stored within employee's files, folders or local non-cloud storage is the responsibility of the employee to destroy according to the retention schedule and data destruction procedures.
    - ABC staff receive training and reminders about their records and destruction obligations. All information will be securely and irreversibly disposed of/destroyed in accordance with applicable ABC policies and procedures, IRS, AICPA, SEC, Treasury and NIST regulations and guidelines,

- Administrative and technical safeguards for protecting PI
    - ABC's M365 implementation is not accessible to anyone outside ABC. The principle of least privilege is used to grant access to ABC staff and contractors, and user actions are tracked in the M365 audit logs.
    - All potential ABC staff and contractors are subject to background investigations and suitability reviews in accordance with HR policies and procedures. Prior to receiving access to ABC's network, all users must agree to the ABC Acceptable Use Policy, which includes consent to monitoring and restrictions on data usage.
    - Before accessing M365, these individuals must first attend new employee orientation and successfully complete ABC's Information Security Awareness and Privacy training. All staff must annually acknowledge procedures for handling PII – including minimizing PII – and attest that all PII maintained by the individual has been properly secured and accounted for as part of ABC's annual privacy and security training.
      ABC does not currently use Phishing or other type of social engineering testing as part of their security awareness program.

- ABC allows remote access on BYOD for designated employees. The access is limited to Outlook Web Access (OWA) and Teams.
- ABC user's computers are configured to automatically attach to the Microsoft Azure cloud infrastructure. The default configuration is for users to automatically save files in that environment.
- Windows Defender is installed by default on all ABC user's Windows PCs. It is set to automatically update and scan for known malware.
- ABC does not use PII to conduct M365 system testing, training, or research. Procedures are in place to ensure any PII is scrubbed or de-identified prior to use in testing or training.
- The ABC website is separately maintained outside of the M365 infrastructure. ABC does not use M365 products or services to collect information directly from the public through their public website.
  ABC's M365 configuration is an intranet site accessible through the ABC network, and only ABC staff and contractors have access to it. Session and persistent cookies keep M365 from timing out while a user is logged into it, but these cookies are used for internal purposes only. M365 does not collect information directly from the public.
- All ABC employees and designated users must have an ABC account using the Microsoft Authenticator app to access the ABC M365 environment.
- ABC's user identity management processes include authentication with Active Directory (AD) to control and manage access restrictions to authorized personnel on an official need-to-know basis. The ABC utilizes a combination of technical and operational controls to reduce risk in the M365 environment, such as encryption, passwords, audit logs, firewalls, malware identification, and data loss prevention policies.
- As a FedRAMP-approved cloud service provider, Microsoft undergoes regular reviews of its security controls.
- The contract between ABC and M365 does not allow the service provider to access, review, audit, transmit, or store ABC data, which minimizes privacy risks from the vendor source.
- A risk exists that internal ABC employees could accidentally or maliciously share customer PI with unauthorized persons using M365 applications.
  This is mitigated through access controls and employee security awareness training.
- User access is managed through ABC's Active Directory (AD) infrastructure, which uniquely identifies, authenticates, and applies permissions to authorized user sessions based on ABC policies and procedures. This allows the ABC to leverage organizational multi-factor authentication solutions, Microsoft Authenticator, already deployed to meet internal identification and authentication requirements. The use of AD also allows automatic enforcement of certain policies and requirements, such as password complexity and maximum log-in attempts, for organizational users.
- ABC security policy states a requirement for system logging, monitoring and alerting, but it has yet to be implemented with the M365 environment. The plan is to purchase and implement Microsoft Sentinel within the next 6-9 months.
- IT has monitoring in place for Microsoft security bulletins and procedures to automatically update systems and applications using Intune. There is no reporting or

alerting on computer systems or applications that may be missing Microsoft patches or updates.

Findings:

- The ABC security and privacy policies were last updated to follow the NIST CSF requirements. When interviewing the DPO, they stated a goal of updating the policies to include the NIST PF.
- In reviewing ABCs policies and procedures, you note that they don't have a security or privacy risk management procedure or vulnerability management plan. Risks are generally informally handled depending on the impacted Director. Microsoft patches and updates are the primary risks documented within the ABC Help Desk ticketing system. There is no vulnerability scanning of the infrastructure outside of standard Microsoft patching analysis. Additionally, changes to the environment are at the complete discretion of the IT manager with little oversight.
- ABC employees are able to send email and documents containing PI through the M365 environment. In your investigation, you determine Data Loss Protection (DLP) is not fully implemented nor configured within the Microsoft 365 environment.
  The IT Manager has recommended ABC consider purchasing Microsoft 365 Security & Compliance or upgrading to a higher tier product suite with advanced security, compliance and DLP functionality.
- In your investigation, you determined that employees (especially remote) often back up files to a personal USB removable storage drive. These drives are not controlled by IT and may contain M365 application files with PII. Employees do this so they can work from home.
- While all endpoint Windows systems have Microsoft 365 Defender installed, the centralized portal is not consistently monitored by the IT Manager. It's been noted that there have been missed alerts often that occur in the middle of the night.
- There is no confirmation that system and application updates are applied consistently across the infrastructure.
- ABC has a shared folder accessible to all within the company. While most of the files are internal memos, you determined some potentially may contain customer PII. (e.g., A Sales contact list with client names, addresses, phone numbers, birth dates, etc.). These documents are not marked with a classification.
- Employees are required to receive annual security and privacy training and certify attendance. In reviewing the training records, you've found 2 senior executives and 10 temporary contractors who have not completed it within the past year.
- Groups are used to limit access to file shares, SharePoint and Teams environments. During your interviews, you find it's up to each manager to review access to those environments. There are multiple file shares that haven't been reviewed in over 2 years and employees with old access based on previous job roles.
- In conducting an access review of a file share containing spreadsheets with PII, it was determined 6 temporary workers had maintained access even though their contract expired 2 months ago. When asked, the responsible manager replied, "I keep their access open just in case we need them for an emergency request."
- There has not been specific testing nor training on the ABC Incident Response (IR) plan. When asked, the IT Manager claims that a recent ransomware scare should count as IT testing / training.