CURRENT & EMERGING TECHNOLOGIES

CONFERENCE

Current and Emerging Technologies Conference

Creating a Technology Solutions Infrastructure

Presenter: Robert Powell

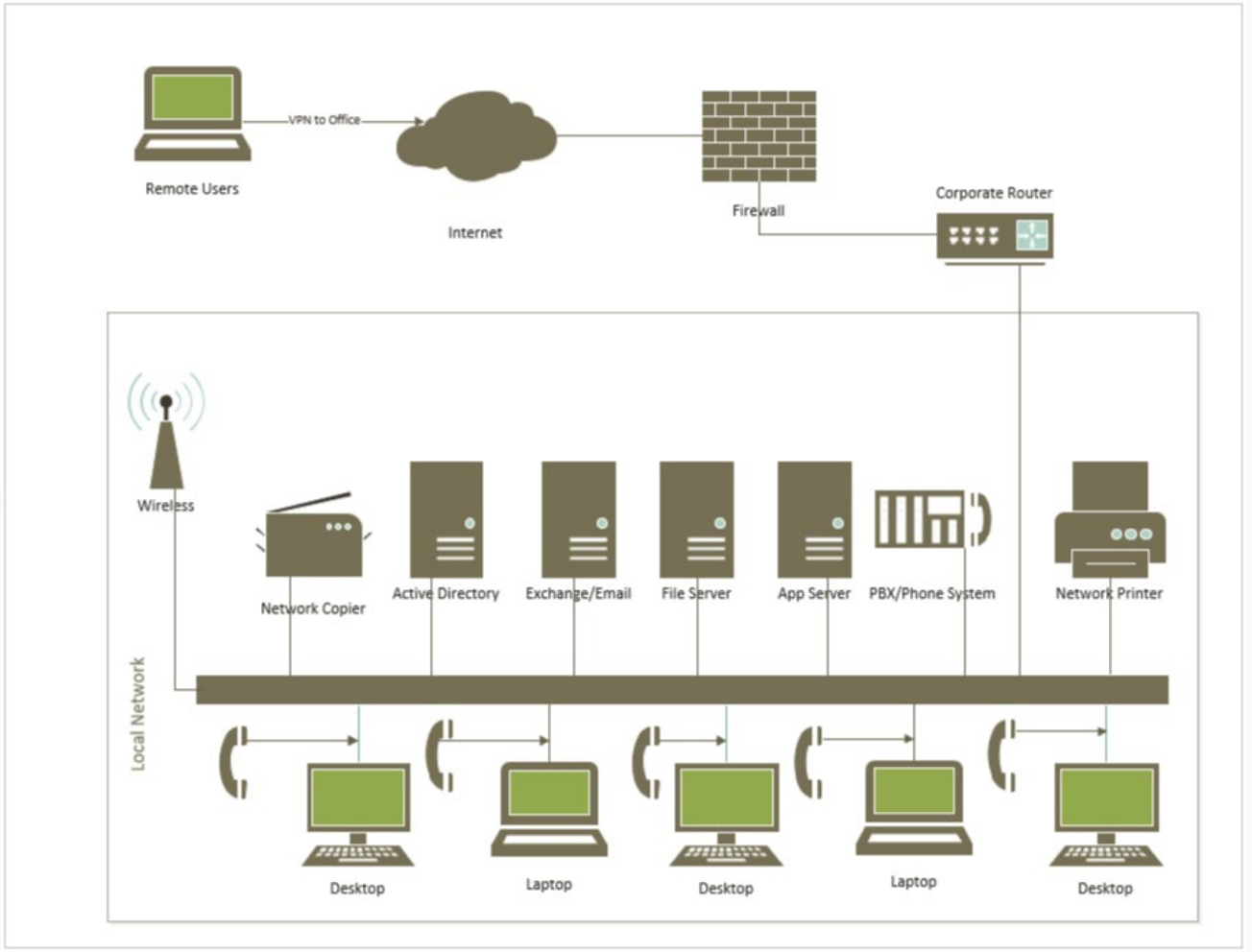
CEMTC – TOPICS

- Core Components of a Technology Infrastructure
- Cyber Security and Components
- Assessing Your Technology Infrastructure

Core Components of a Technology Infrastructure

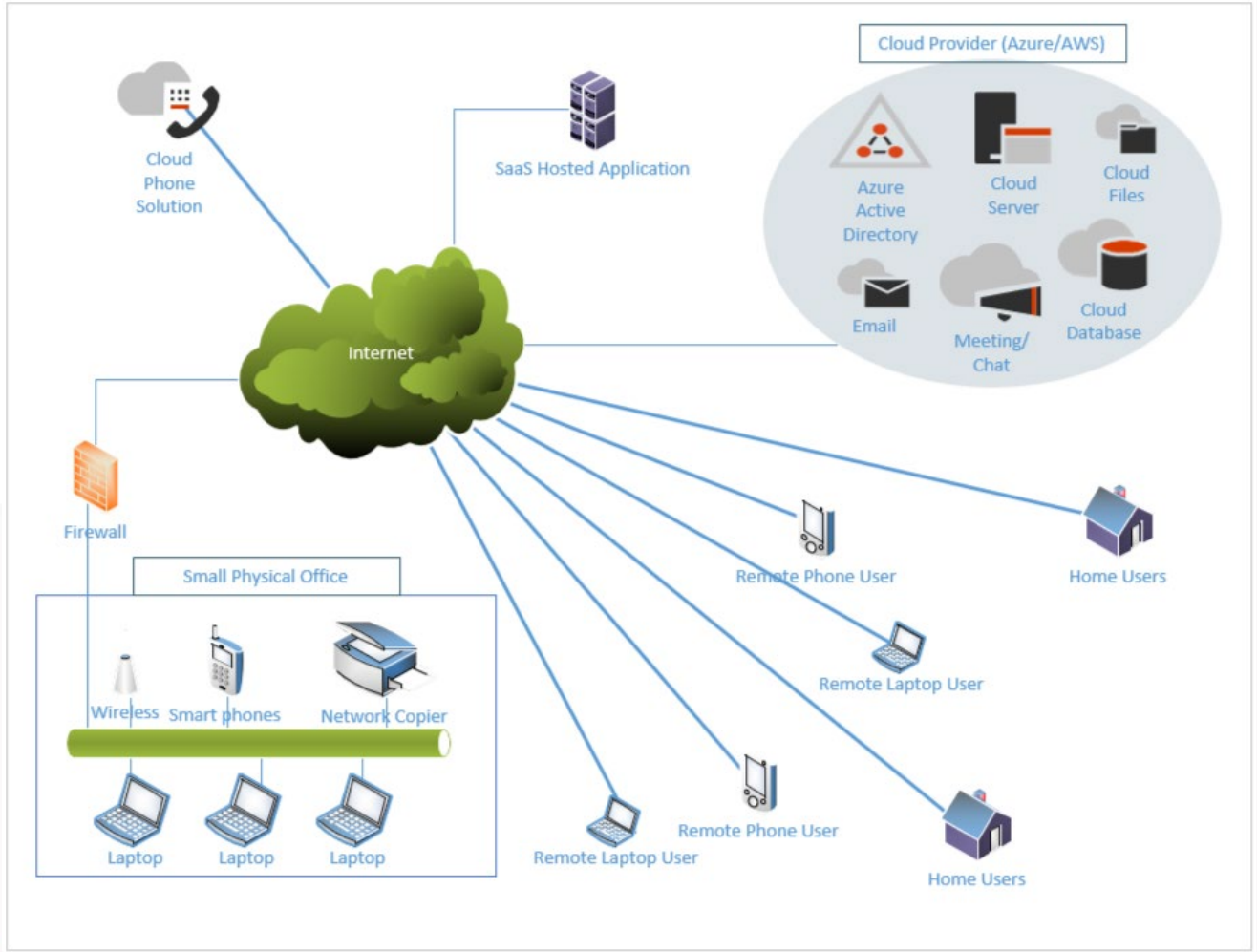
Legacy Technology

- Most users worked inside an office.
- Most applications and servers were physically on the local network.



Today's Technology

- Office space is smaller and shared.
- Users work remotely permanently or in a hybrid model.
- Most applications and servers are hosted in the cloud.



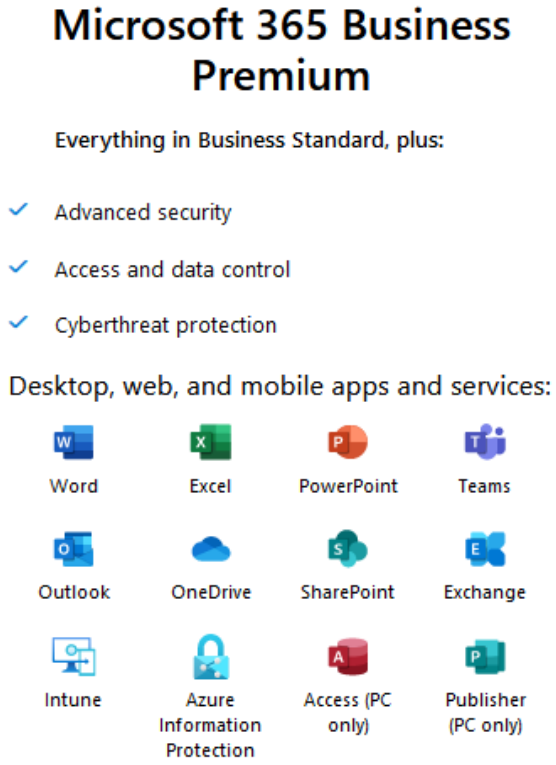
Core Elements for Today's Network

- Physical Office Locations
  - Internet Connectivity
    - Preferably 2 failover connections with different providers
  - Network Switch(es)
  - Wireless Access Points
  - Firewall with Next Gen Security Suite
  - Uninterruptible Power Supply (UPS)

Core Elements for Today's Technology

- Microsoft 365
  - Hosted Exchange Email
  - Teams for Meetings and Chat
  - OneDrive and SharePoint for File Storage
  - Microsoft Office Licensing
  - Active Directory

- Microsoft 365 Plan Recommendation for SMB



Core Elements for Today's Technology

- Line of Business Applications
  - 1st Option and Preference – Hosted and maintained in a SaaS model by the software vendor.
  - 2nd Option – Hosted as a service or as a virtual server running at a cloud provider, such as AWS or Azure.

Core Elements for Today's Technology

- Business Phone Solution
  - Hosted at a Cloud Provider
    - Microsoft Teams
    - Zoom
    - Sangoma Digium
  - End User Experience
    - Fewer users have a traditional desk phone
    - Most users are using a soft phone app running on their mobile phone and/or their computer.

Core Elements for Today's Technology

- Management and Monitoring Tools
  - Azure Active Directory
    - User and computer management
    - Policy management
  - Remote Management and Monitoring Tool
    - Microsoft Intune
    - Datto RMM
    - Kaseya VSA

Core Elements for Today's Technology

- Cyber Insurance
  - Cyber insurance is a type of general liability insurance related to insurance companies against cyberattacks and hacking.
  - Cyber insurance typically covers:
    - Network security and privacy
    - Media liability
    - Errors and omissions
    - Network business interruptions
- Business IT Policies – Acceptable Use, Breach Notification, Remote Access, Privacy, etc.
  - These should be regularly reviewed and enforced.

Cyber Security and Components

Cyber Attacks

- Most Common Attacks
  - Ransomware and Phishing (i.e., spear, smish and vish).
- Myths
  - My business is too small to be attacked.
  - A good password is enough.
  - My computer updates automatically.
  - A good antivirus solution alone will keep me protected.
  - A hacker will be quickly in and out of my network.

Cyber Attacks

Cyber Insurance Requirements and Core Security Elements

- Endpoint Detection and Remediation (EDR) and Managed Detection and Response (MDR)
  - EDR – Beyond traditional antivirus. Includes artificial intelligence technology to detect and prevent suspicious activity in real time, not just depend upon outdated virus definitions.
  - MDR – Uses EDR technology, but also adds the functionality of a Security Operations Center (SOC) to monitor and address threats.
  - Either way, both solutions should be managed and logged to a central portal that performs software and patch updates and captures event logs.

Cyber Insurance Requirements and Core Security Elements

- Multifactor Authentication (MFA)
  - Uses multiple forms of authentication, beyond the traditional username/password. Most common are adding the use of an OTP (one time password) sent to your phone or an app on your phone or email. The use of cards or secure tokens are frequently used.
  - Areas that must be secured by MFA:
    - Email, whether on premise or in the cloud
    - Servers
    - VPN access to company's network and data
    - Other remote access solutions, such as Citrix or Remote Desktop

Cyber Insurance Requirements and Core Security Elements

- Regular Patching
  - Includes:
    - Operating System security and feature patching
    - Application (Microsoft Office, Adobe Acrobat, etc.) security and feature patching
  - Must be centrally managed and monitored to ensure that all systems and applications are fully up to date.
  - Recommend weekly patching.
  - Capture patching logs.

Cyber Insurance Requirements and Core Security Elements

- Backups and Disaster Recovery
  - Solutions must cover the following:
    - Be protected from threats like ransomware, hardware failure and natural disaster.
    - Provide onsite and offsite recovery methods.
    - Image backups are preferred for quick system recovery.
    - Daily backup monitoring for success and remediation.
    - Quarterly testing of system and file recovery.

Cyber Insurance Requirements and Core Security Elements

- End User Training
  - Most infiltrations occur due to poor user decisions
    - Failing to recognize a phishing email and clicking on a link, opening an attachment or submitting a payment.
    - Poor web browsing habits.
  - Recommended Training
    - Regular email phish testing and reporting
    - Short security awareness videos based upon phishing failures.
    - Annual security awareness training across the company. Completion is mandatory. This includes acceptance of all company security policies (acceptable use, etc.) , along with industry security best practices.

Cyber Insurance Requirements and Core Security Elements

- User Permissions and Accounts
  - Remove local administrative rights from users' computers.
  - All IT Team members should have a separate account for administrative functions from their daily work account.
  - Privileged administrative accounts should be monitored and passwords should be regularly changed.
  - Membership to administrative groups (i.e., Domain Admins) should be regularly audited.
  - Permissions to critical and sensitive files should be regularly audited and adjusted.
  - Enforce strong passphrases (not passwords)

Cyber Insurance Requirements and Core Security Elements

- Additional Recommendations
  - Perform regular internal scans utilizing security software or a third party to check for security gaps
    - Rapid Fire Tools
    - CyberCNS
  - Use a zero-trust solution for locking down machines to just approved applications and activity.
    - Microsoft AppLocker
    - ThreatLocker
  - Use a Cybersecurity SIEM (Security Information & Event Management)
    - Arctic Wolf
    - ConnectWise SIEM (Perch)

Assessing Your Technology Infrastructure

IT Assessment

- Assessment Types
  - General IT Assessment for Best Practices
    - Evaluates all of the items above for general best practices and best security practices. Additional items could involve:
      - IT staffing evaluation
      - Policies and procedures review
      - Contract review
      - Vendor review
  - Specific compliance assessment, driven by industry or specific business need
    - Examples: HIPAA, PCI, SOC 2, CMMC

Question Review

Thank you for attending this session

If you have any questions about any of these topics, please reach out to me.

Robert Powell

Robert.powell@lbmc.com

615-309-2456

https://www.lbmctech.com

LBMC TECH