THE TIPS, TOOLS AND TALENT TO EXPAND IT SUPPORT TO MOBILE USERS

Do you face challenges supporting end users in this ever-growing mobile workforce? A panel of peers is here to help and will tackle a variety of support scenarios in which the goals are providing efficient, secure and cost-effective IT assistance to end users on the go. Learn about the tips, tools and talent needed to effectively expand IT support to mobile users.

#ILTAG145

Session Participant Polls

- Does your firm currently support BYOD with reimbursement?
  - yes or no
- Does your firm offer the option of either a corporate device or employee-owned device for mobile phones?
  - yes or no
- Is it important for your firm to containerize business related content and separate from a user's personal content?
  - yes or no
- Does your firm already have an approved policy specifying who (exempt, non-exempt, staff, lawyer, etc.) is approved to work remotely?
  - yes or no
- Would your firm consider a full BYOD policy that includes all technology required for a job function (computer, phone, tablet, etc.)
  - yes or no

SPEAKERS

Frank Ziller

CIO

Intelliteach

Ken Oregon

CIO

Gardere Wynne Sewell, LLP

Eric Haas

Director, Customer Experience

Hinshaw & Culbertson, LLP

Statistics and Facts to Consider

- 80% of internet users own a smartphone
- 20% of 19-34 Millennials don't use a desktop at all
- By 2020 Millennials will constitute 50% of global workforce
- 70% of professionals will do some work from their personal smart phone\tablet by 2018
- 80% of workers access corporate documents on the move using mobile devices (laptop, phone, tablet)
- Over 50% of smartphone users grab their smartphone immediately after waking up
- According to IDC, by 2020 mobile workers will make up nearly 75% of workforce

Key Considerations for Supporting the Mobile Workforce

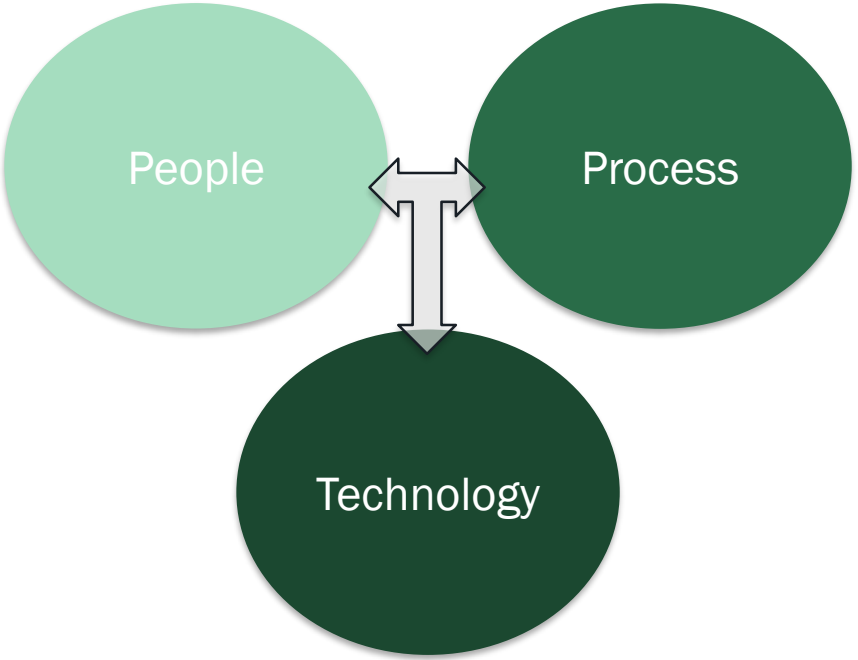
- Mobile operating systems may not offer all the functionality of traditional laptop operating systems; however, they are equally complex to configure, manage and support
- Both MDM & PCM tools are increasingly complex
- Security & compliance considerations are rapidly changing and evolving
- Single pane of glass for all end points (would be nice, right?)
- User behavior is typically governed by a combination of technology and policy
- End user productivity and efficiency is paramount

BYOD Specific Considerations

- Employ tool(s) to manage heterogeneous population of devices
- Employ easy to replicate policy across heterogeneous population of devices
- Containerize data in some fashion
- End user agreements & policies

A Foundation for Success

1. People
2. Process
3. Technology



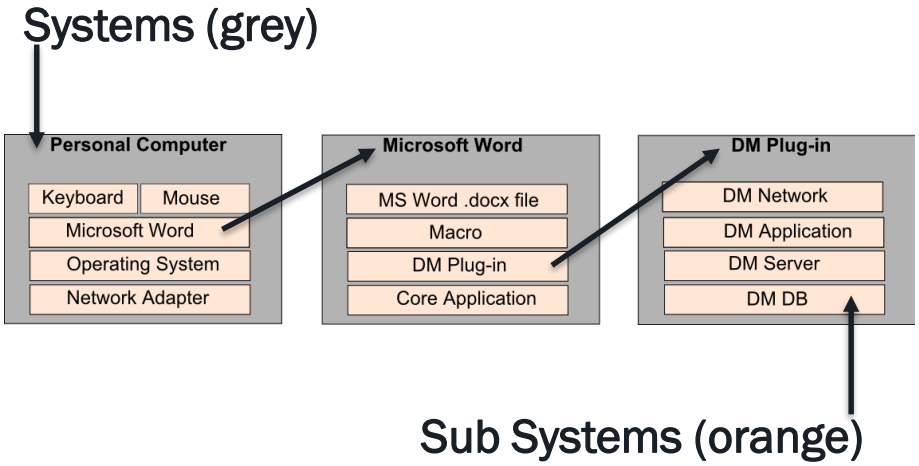
Your People & AASkE

- Attitude
- Aptitude
- Skills
- Experience

- End point support experience
- Active Directory & group policy
- Broad range of application support experiences with one or two areas of expertise
- Multiple desktop & mobile OS experience
- PC and\or Mobile Device Management tool experience
- Strong problem solving skillset

Employing ‘Systems Thinking’

- States that any system is comprised of a subset of smaller systems with inputs\outputs
- Useful for understanding how a given system functions
- Indispensable in isolating a problem in a break\fix situation – divide problem into smaller systems until isolated



PANEL DISCUSSION
TRAINING, EDUCATION & SUPPORT

Define Expected Experience

- Understand what requirements there are to work remotely
  - Able to place calls? Email access? Create, edit, review documents?
- Describe and outline what it would be like to work remotely
  - Physical desk phone? Laptop computer? Apps on mobile device?
- Compare to existing functionality and prioritize what needs to be added/reconfigured to meet requirements and expectations
  - Edge servers? VPN or Citrix? BYOD?
- End user support expectations
  - Service Desk, Self s\Service, etc.

Formulate An Effective Policy

- Whatever you roll out to some will have to be given to others, a solid policy will help to dictate who can get what access and desired functionality
- The policy should address things like security requirements, what the company will provide/not provide, what roles are deemed “work remotely” capable, etc.
- A policy agreement should be signed by every individual who desires to work from a remote location.

End User Agreements

- Likely two policies
  - Corporate owned devices
  - Employee owned devices a/k/a BYOD
- Use policy to govern end user behavior where a tool\technology may not be available or practical to deploy

PANEL DISCUSSION
END USER POLICY & AGREEMENTS

Formulating Best Practices

- Need predictability in configuration
  - So device behavior is predictable
- Consistent security policy to mitigate risk
  - Devices are in the wild
  - Heterogeneous device population to support
- Consistency results in efficiency
- Audit and compliance benefits – feedback loop required

Foundational Security Strategy
Protecting User Experience and Data

1. Protect Perimeter
   – Internet connectivity and the cloud for SaaS offerings
2. Control End Points
   – ActiveSync, PCM/MDM tools, Group Policy, AV, etc.
3. Visibility into Infrastructure and Applications
   – Tools and process for proactive and reactive monitoring
   – Look for AI\ML for ‘security analyst in a box’

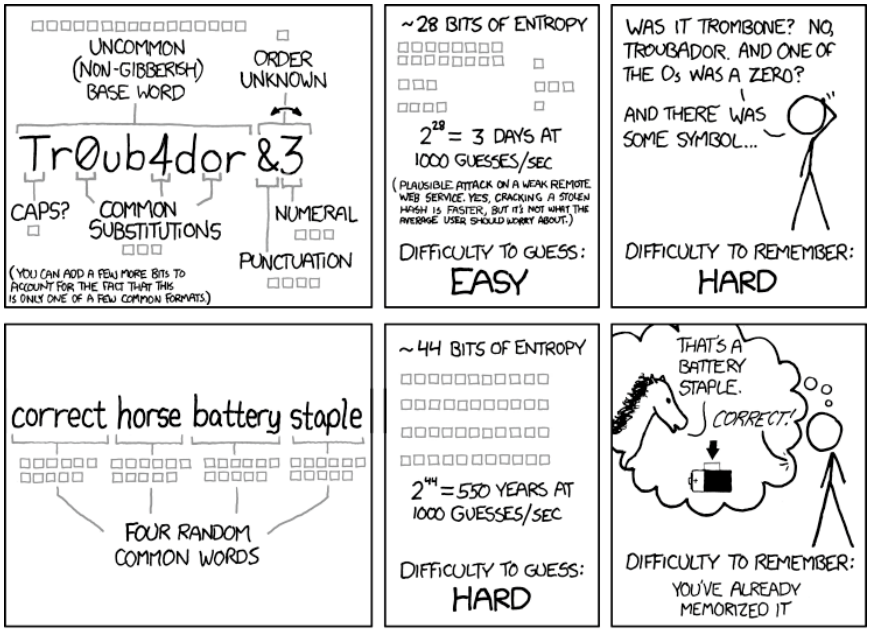
Security & Compliance – Control End Points

- Security with convenience is a paradox
- Keep in mind – these devices are typically in the wild which means they are vulnerable; primary vector for malware
- Many tools with different capabilities required
- Regulatory considerations

PANEL DISCUSSION
A NEW APPROACH TO PASSWORD POLICY

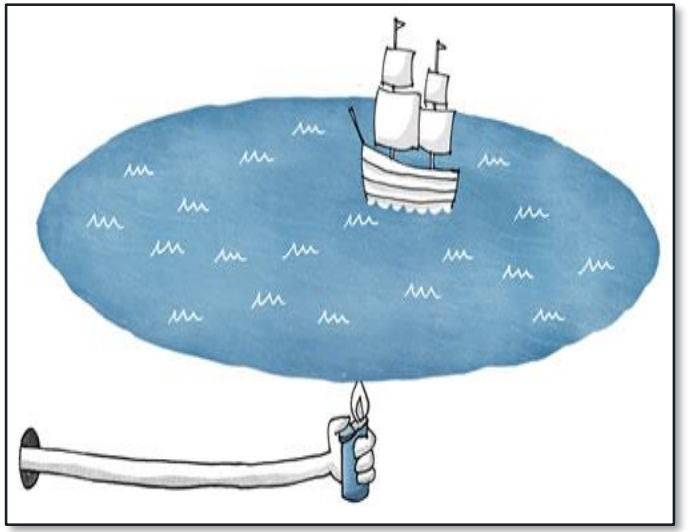
PASSWORD SECURITY POLICY

A FRESH APPROACH



PCM\MDM Tool Deployments

- Take an iterative approach
  1. Email is a great starting point
  2. Inventory is key ingredient
  3. Device policy – layers are key
  4. Network access controls
  5. Data\content management
  6. Application management



Tip! Avoid boiling the ocean

Access to email & content [MDM]

- Email
  - Deploy MS ActiveSync Policies
  - Native mobile OS email clients vs. third party email clients
- Content Distribution and Access
  - Distribution mechanism
  - Access control
  - Limits data leakage

Inventory

- Enables the tracking of what data is on which device(s) by which employee
- Software Licensing
- Last Known Configuration Data
- Identify potential configuration issues
- Identify current and future security risk

Remote Control & Self Service: Support Accelerators

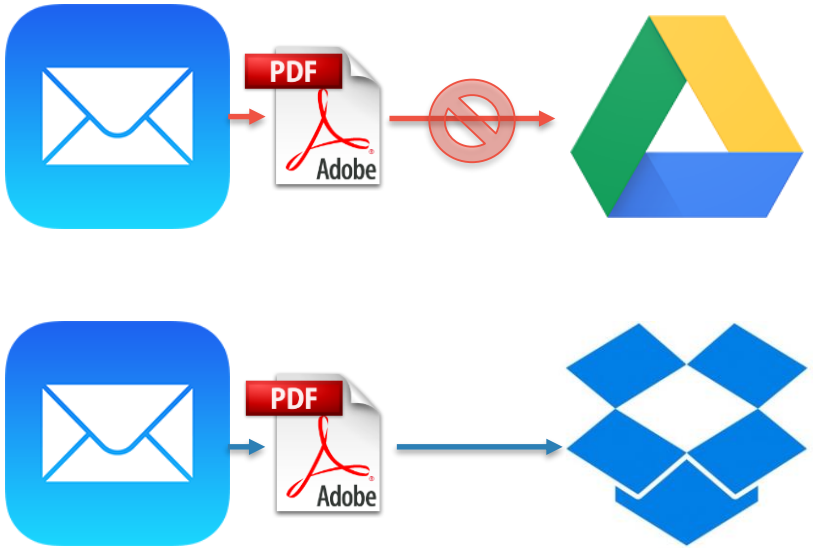
- PCM tools typically offer some form of remote control
- 3rd party PC remote control support tools also available
- MS Windows Remote Desktop common for Windows PCs
- MDM tools typically do not offer remote control
  - 3rd Party Options Available; limited functionality
- Self-Service Portals
  - Intuitive interface imperative
  - Short, succinct answers imperative
    - Video and bullet-pointed instructions shorten answer\resolution time

Secure Access to Internal Applications

- Protected web browser
  - Great for accessing web applications hosted on internal networks without a OS based VPN or law firm issued asset
- Multifactor authentication recommended
- Traditional Corporate VPNs
  - Additional benefits
    - Access to non-web applications
    - Standardized approach for end point access: Tablets, Phones, Laptops, PCs
  - Multifactor Authentication recommended

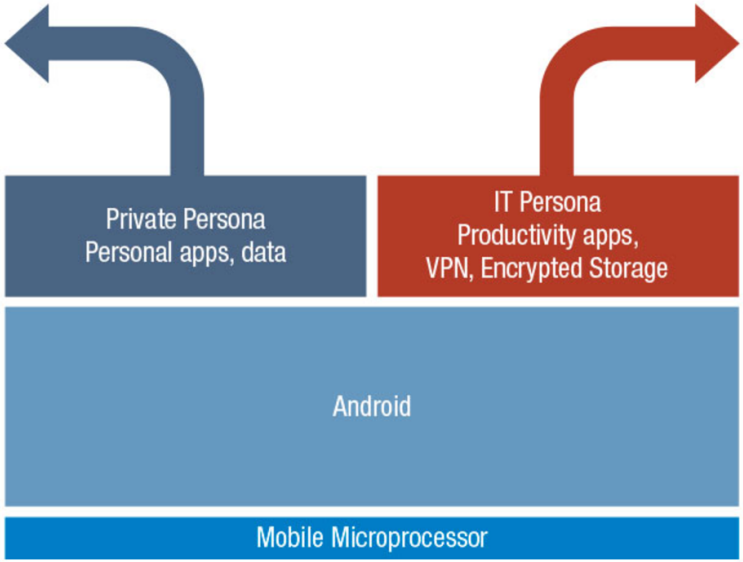
Data Passed Between Mobile Apps [MDM]

- Governs how an end user can consume and manage data
- Facilitates what mobile apps can interact with corporate data



Sandboxes [MDM]

- Determines how an end user can consume and manage data
- Specifies a limited number of safe places where data can be stored



File Sharing

- Can replace traditional user file shares; perhaps group shares depending on tool
  - Opportunity for expense reduction
  - Operational efficiencies
- Can compliment Office365 on all devices
- Strength in offering ubiquitous access to unstructured data for multiple platforms
  - One client for Windows, Mac, IOS & Android
- Cloud, on-premises & hybrid offerings

PANEL DISCUSSION - FILE SHARING

GENERAL Q & A