

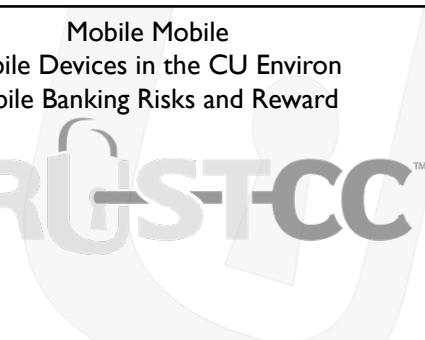
Tom Schauer
TrustCC
tschauer@trustcc.com
253.468.9750 - cell



Copyright TrustCC. All Rights Reserved.




Mobile Mobile
Mobile Devices in the CU Environ
Mobile Banking Risks and Reward



TRUSTCC™

Copyright TrustCC. All Rights Reserved.

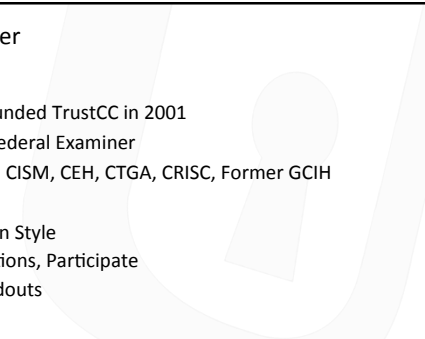


Tom Schauer


- ✓ Since 1986
- ✓ TrustCC Founded TrustCC in 2001
- ✓ State and Federal Examiner
- ✓ CISSP, CISA, CISM, CEH, CTGA, CRISC, Former GCIH

✓ Presentation Style

- Ask Questions, Participate
- Your Handouts



Copyright TrustCC. All Rights Reserved.



Mobile Device Proliferation

“The Number of Mobile Devices will Exceed the World’s Population By 2012”

Latest trends indicate “business users” have both tablet and smart phone.

Copyright TrustCC. All Rights Reserved.



Legitimate Business Purposes

- ✓Email, Contacts and Calendar
 - Contacts Sensitive Data
 - ✓Names, Addresses, Emails, Phone Numbers
 - Email Sensitive Data
 - ✓Attachments containing all sorts of data

Copyright TrustCC. All Rights Reserved.



Legitimate Business Purposes

- ✓Productivity (Docs, Web)
 - Portable Office
 - ✓Word, Excel, PowerPoint
 - CRM
 - ✓Sales
 - ✓Loan Origination
 - ✓New Accounts
 - Attend Webinars and Meetings on the Road

Copyright TrustCC. All Rights Reserved.



Risks of Mobile

- ✓ Nobody wants to carry two smart phone, pay two service plans, etc.
- ✓ Sensitive Non-Public Personal Information (NPPI) about the Credit Union and it's members now proliferates through these personally owned devices.

Copyright TruSTCC. All Rights Reserved.



User Failure

- ✓ Failure to treat smart phone like a tiny computer.
- ✓ Mobile malware is on the rise yet most users have no malware protection
- ✓ Willingness to download apps of unknown provenance.
- ✓ Insecure Wi-Fi
- ✓ Smishing/Phishing

Copyright TruSTCC. All Rights Reserved.



Jail-broken/Rooted Devices

- ✓ Jail-broken/Rooted – intentionally hacked by owner to give the owner administrative control over the device's operating system and "increase" functionality.
- ✓ Jail-broken/Rooted devices lose all built in integrity and security advantages

Copyright TruSTCC. All Rights Reserved.



Separate Ecosystems

- ✓ Android Market
 - Google Play
 - Slow adoption of upgraded OS
- ✓ Apple App Store
 - App Store
 - Strong adoption of upgraded OS

Copyright TrustCC. All Rights Reserved.



iOS vs. Android Security Provisions

- ✓ Very VERY Immature Operating Systems
 - Traditional Access Controls
 - ✓ Both support passwords, lock outs and time outs though Android 2.x is limited
 - ✓ Pattern and 4 Digit PIN barely offer benefit
 - ✓ Users are resistant to use these controls
- ✓ Difficult to validate/verify security settings

Copyright TrustCC. All Rights Reserved.



iOS vs. Android Security Provisions


- ✓ Encryption
 - Apple has 256 bit hardware encryption and secondary encryption on some data (email)
 - ✓ Enabled by setting a passcode
 - Android has implemented hardware encryption with latest OS and devices
 - ✓ Not Automatic

Copyright TrustCC. All Rights Reserved.




iOS vs. Android Security Provisions

- ✓Application Provenance
 - Apple
 - ✓closed market
 - ✓Tests apps for malicious behavior or violations of their policies
 - ✓Apps signed by Apple issued Developer ID
 - Android
 - ✓Open market, no tests
 - ✓Self signed apps


Copyright TruSec, All Rights Reserved. 

iOS vs. Android Security Provisions


- ✓Permissions
 - Apple
 - ✓Not reliant on a permissions model
 - Android
 - ✓Users must accept permissions.
 - ✓Do users understand the permissions they grant? Clearly they do not!

Copyright TruSec, All Rights Reserved. 

iOS vs. Android Security Provisions



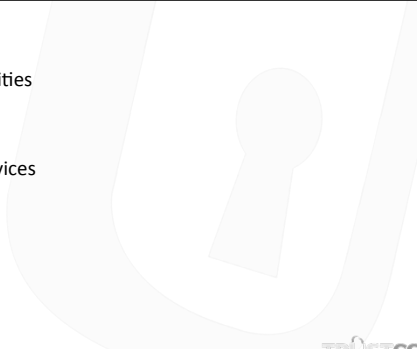
- ✓Permissions

Copyright TruSec, All Rights Reserved. 

Upcoming

- ✓ More capabilities
- ✓ NFC

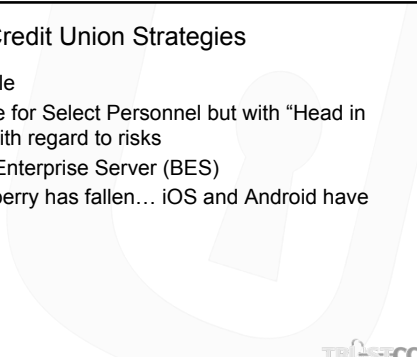
- ✓ Wearable devices



Copyright TrustCC. All Rights Reserved.

Historical Credit Union Strategies

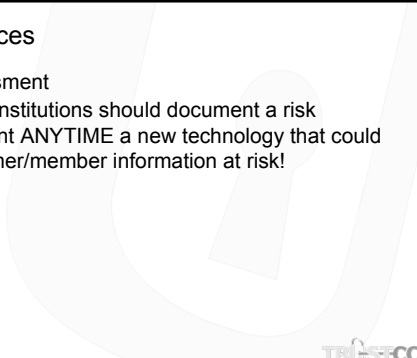
- ✓ Ignore Mobile
- ✓ Allow Mobile for Select Personnel but with "Head in the Sand" with regard to risks
- ✓ Blackberry Enterprise Server (BES)
 - But Blackberry has fallen... iOS and Android have risen



Copyright TrustCC. All Rights Reserved.

Best Practices

- ✓ Risk Assessment
 - Financial Institutions should document a risk assessment ANYTIME a new technology that could put customer/member information at risk!



Copyright TrustCC. All Rights Reserved.

Best Practices

- ✓ Acceptable Use Agreements
 - Require employees to sign an acceptable use agreement stipulating their responsibilities
 - The acceptable use agreement should be based upon a well written policy

Copyright TriSTCC. All Rights Reserved.



Best Practices

- ✓ Employee Training
 - Personnel with Mobile (smartphone, tablet or laptop) should undergo specific training for these devices.
 - ✓ Risk of Public Internet Connections
 - ✓ Authentication AV, Encryption
 - ✓ Theft of Mobile
 - ✓ Cloud Services and Applications/Software

Copyright TriSTCC. All Rights Reserved.



Best Practices

- ✓ Inventory Regularly
 - Mobile devices, including laptops, can go missing and may not be noticed.

Copyright TriSTCC. All Rights Reserved.



BYOD – Bring Your Own Device

✓Risks and Rewards

- Employees are more likely to have increased productivity through mobile with a phone they choose
- Employee owned devices may be jail-broken or may have apps that could lead to compromise
- Even with a signed agreement, you may not be able to legally wipe a privately owned device

- Can you prevent BYOD?

Copyright TruCC. All Rights Reserved.



Solutions

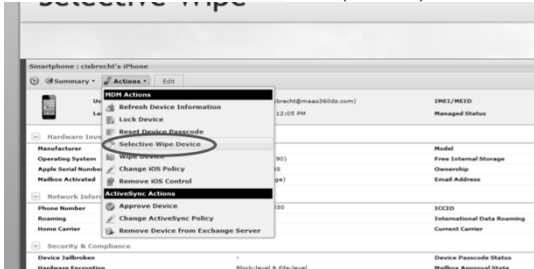
- ✓Exchange 2010
 - Allow Sync of eMail, Calendar, Contacts
 - Remote Wipe and PIN enforcement

- ✓Mobile Device Management (MDM)
 - More Visibility and Greater Cross-Platform
 - Increased Security Functionality
 - Location and Activity Tracking
 - Jail-broken or Rooted Detection
 - Maas360 and Mobile Iron

Copyright TruCC. All Rights Reserved.



Solutions – How Cloud MDM (MaaS360) works...



Cost \$10-\$20 per month per device.

Copyright TruCC. All Rights Reserved.



BYOD –

- ✓ Important Operational Controls
 - Enforcement of Policy
 - Selective Wipe
 - Application White-listing
 - Notification when lost or stolen
 - Enforce Encryption

Copyright TrustCC. All Rights Reserved.



Best Practices

- ✓ Protect Administrative Privileges
 - Enforce traditional access controls such as passwords, inactivity timeouts, and device lock-outs.
 - Enforce what applications can and cannot be installed.
 - Do NOT allow Jail-broken or Rooted Devices

Copyright TrustCC. All Rights Reserved.



How to Audit – Basic Audit Procedures

- ✓ Review Policies, Practices, Risk Assessment
- ✓ Sample Devices and Test for Compliance with Policies
- ✓ Sample Users to Validate Training and Signature on Acceptable Use
- ✓ Test Wipe Procedures

Copyright TrustCC. All Rights Reserved.





Mobile Banking

- ✓28% of mobile phone owners have used mobile banking in the last 12 months. Up from 21% a year earlier.
- ✓87% of consumers that bank via mobile use mobile to check account balances or recent transaction.
- ✓21% have used mobile to deposit a check.
- ✓36% say they don't know how safe it is to bank via mobile

- ✓54% of consumers feel their banking needs are met without the use of mobile.

Copyright TrustCC. All Rights Reserved.

What a Mobile Risk Assessment Look Like...

December 2012

In 2005, the Federal Financial Institution Examination Council (FFIEC) published authentication guidance titled *Authentication in an Internet Banking Environment*. The FFIEC then published *Supplemental Guidance on Internet Banking Authentication* to all federally insured financial institutions in December 2010. The guidance referenced above requires that financial institutions perform an Internet Banking Risk assessment to ensure a layered security control environment exists to appropriately authenticate consumers utilizing electronic banking systems – primarily Internet Banking. The risk assessment that follows considers reasonable foreseeable threats, the impact and likelihood of the threat, and mitigating controls.

Funstrom Credit Union's Internet Banking System
 The Financial Institution's Internet banking system is outsourced to **CompanyA** and **CompanyB** provides bill payment capabilities. Internet Banking is accessible through a web browser and a mobile banking interface. The combined capabilities for consumers are listed below. (o) designates online, (b) designates both online and mobile.

1. account management (address change, pw change, etc.) (o)
2. account inquiry (b)
3. intra-account transfers (of same ownership) (b)
4. inter-bank transfers (of same ownership) (o)
5. p to p transfers (e, m by Jan 2013)
6. bill pay - add/remove payee (o)
7. bill pay - payment (b)
8. loan payments (b)
9. e-deposits (b)
10. check orders (o)
11. e-statements (o)
12. stop payments (b)
13. personal financial management software (o)
14. image check images (b)

Copyright TrustCC. All Rights Reserved.
