Tom Schauer TrustCC tschauer@trustcc.com 253.468.9750 - cell

pyright TrustCC. All Rights Reserve

TRESTCC

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

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

yright TrustCC. All Rights Reserve



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.	
Consist Note: All Bell Report.	
Copyright TrustEC. All Rights Sources.	
	_
Legitimate Business Purposes	
✓Email, Contacts and Calendar	
> Contacts Sensitive Data	
✓ Names, Addresses, Emails, Phone Numbers > Email Sensitive Data	
✓Attachments containing all sorts of data	
тинэнсс	
Copyright Tradition All Rights Reserved.	1
	1
Legitimate Business Purposes	
✓Productivity (Docs, Web)	
≻ Portable Office✓ Word, Excel, PowerPoint	
> CRM ✓ Sales	
✓Loan Origination ✓New Accounts	
> Attend Webinars and Meetings on the Road	
Compatibility of Spirit Interest.	
mpp que comme co approximativa	1

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.	
TRUSTCC	
Copyright houte. All Rights Research	
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 TransCC. All Registratures &	
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	
	-

Separate Ecosystems	
✓Android Market	
≽ Google Play	
➤ Slow adoption of upgraded OS	
✓Apple App Store	
> App Store	-
> Strong adoption of upgraded OS	
Copyright Tradition. All Rights Reserved.	
iOS vs. Android Security Provisions	
100 vs. 7 that old occurry 1 Tovisions	
✓ 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	
V Osers are resistant to use these controls	
(Difficult to wall date (south a country and this are	
✓Difficult to validate/verify security settings	
Consist ToniCE. All Relats Reserved.	
зорущи топы. Ат одил липтио.	
iOS vs. Android Security Provisions	-
(Eneryption	
✓ 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 TrackC. 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

TRGSTCC

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!

TRESTCC

iOS vs. Android Security Provisions



Upcoming	
· More capabilities	
✓NFC	
✓Wearable devices	
Appropriat Tractic. All Rights Insered.	
	1
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	
TRESTCC	
	_
Best Practices	
√Risk Assessment	
Financial Institutions should document a risk assessment ANYTIME a new technology that could	
put customer/member information at risk!	

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 TranSCC. 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	
TRESTCC	
Copyright Tool CC. All Rights Reserved.	
Best Practices	
✓Inventory Regularly	
> Mobile devices, including laptops, can go missing	
and may not be noticed.	
Capyright TransCC. 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?

pyright TrustCC. All Rights Reserve

TRESTCC

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

right TrustCC. All Rights Reserve



olution		ud MDM (MaaS	360) WOIKS
Smartphone : cisbre	cht's iPhone		
⊙ @Summary •	Actions • Edit		
Us	MDM Actions 強 Refresh Device Information	sbrecht@maas360dz.com)	IMEI/MEID
La La	Lock Device	12:05 PM	Managed Status
	Reset Device Passcode		
m Hardware Inve	Selective Wipe Device		
Manufacturer Operating System	tin Williams	90)	Hodel Free Internal Storage
Apple Serial Number	Change iOS Policy	50)	Ownership
Mailbox Activated	Remove iOS Control	ge)	Email Address
Network Inform	ActiveSync Actions		
Phone Number	Approve Device	130	ICCID
Roaming	Change ActiveSync Policy		International Data Roamin
Home Carrier	Remove Device from Exchange Ser	ver	Current Carrier
Security & Com	spliance		
Device Jailbroken			Device Passcode Status
Hardware Encryption	n Bloc	cic-level 5. File-level	Hailbox Approval State
_	410.000	r month per de	

BYOD –	
✓Important Operational Controls > Enforcement of Policy	
> Selective Wipe	
≻ Application White-listing≻ Notification when lost or stolen	
> Enforce Encryption	
Carolit Tests. At this lawses.	
Copyright TrusCC: 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	
> DO NOT allow sall-bloker of Rooted Devices	
Copyright TrustCC. All Rights Reserved.	
	1
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	
Carolit Tests, at the lateral	
Copyright TransCC. 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.
- $\checkmark\!21\%$ have used mobile to deposit a check.
- √36% say they don't know how safe it is to bank via mobile
- $\checkmark 54\%$ of consumers feel their banking needs are met without the use of mobile.

pyright TrustCC. All Rights Reserve



What a Mobile Risk Assessment Look Like...

December 2012

in 2005, the Tederal Tinascial Institution Examination Council (FFEC) published authentication guidance tilled Authentication in an internet Banking Terrioriment. The FFEC (Them published Supplemental Guidance on Internet Banking Authentication as differently insured Bancasi Institutions in December 2010. The guidance referenced above requires that filmacial institutions perform an Internet Banking risk assessment to ensure a bigweet security contact evidenment exists is appropriately authentication comment suttings described banking types — juniship internet banking. The risk security contact evidenment exists is appropriately authentication comment suttings described banking stream — juniship internet banking. The risk security contact evidence is a supplemental security of the propriate propriate

The Financial Institution's Internet banking system is outsourced to <u>CompanyA</u> and <u>CompanyB</u> provides bill payment capabilities. Internet Banking in accessible through a web browser and a mobile banking interface. The combined capabilities for consumers are listed below. (o) <u>designates</u> online,

- account management (address change, pw change, etc.) (g
- intra-account transfers (of same ownership) (I
 intra-bank transfers (of same ownership) (I)
- intra-bank transfers (of same ownership)
 p to p transfers (o, m by Jan 2013)
- bill pay add/remove payee
 bill pay payment (b)
- loan payments (I
 e-deposits (b)
 check orders (c)
- 12. stop payments (b)
 13. personal financial management softs
- personal financial manages (b)



Best Practice	Documents Requested	ew Look Like.	Recommendations and	Priority
In Internet Banking Risk Assessment exists and has been updated in the last 12	Internet Banking Risk Assessment (not	An Internet Banking risk assessment has not been performed.	TrustCC recommends that an Internet Banking risk	(H, M, L)
onths	Vender Risk Assessment (Doc_1 Vender_Mgmt_Procedures_MShift) MISRA		assessment should be performed to assess risk and to determine mitigating controls for internet Banking.	
570 User Control Considerations are nsistently performed.	SAS70 and SAS70 User Control Considerations (NTT MShift SAS70, NIT	A SAS70 report from 9/2010 was provided for review.	Effective	
	Social and Security Position Statement MShift and Security Position Statement		Effective	
The vendor contract addresses periodic security assessments of the hosted site and application. The vendor contract addresses their	Vendor Contract Vendor Security Assessment Reports Vendor Security Assessment Reports Vendor ECP and Test Results Vendor Incident Response Plan Braupons for Unautherized Access Vendor Management Policy Vendor and Business Partner Management Policy	Best practices are in place at <u>Funtown</u> Credit Union.	Effective	
Incident Response Plan and notification procedures. The vendors control environment is	Response for Unauthorized Access Vendor Management Policy Vendor and Business Partner Management			
other attestation reports/reviews.				
The procedure for establishing a mobile banking account is well controlled.	Procedure for establishing accounts	Mobile banking accounts are linked to online banking accounts. Procedures for establishing a mobile banking account is well controlled.	Effective	
Members must choose 8 to 12 character passwords and must use a combination of	Configuration Settings for Passwords and other Controls	well controlled. 8-20 character long passwords, alpharumeric but special characters not	TrustCC recommends that passwords be at least 8-12	L
FrustCC. All Rights Reserved.		1		-STO
\A/ba+ a \4ab	ilo Donosit F	Poviou Look	iko	
vviiat a iviot	nie Deposit i	Review Look L	ıke	
Funtown Federal Cred	it Union <u>eDeposits</u> Review	w – November 2012		
Summary:				
TrustCC performed an audit of Mobil Examination Handbook. The key t	le banking <u>eDeposits</u> . The audit program findings follow:	was adapted from the February 2010 F	FIEC Retail Payment System	ns IT
Finding: By policy, eDeposits are	supposed to be limited to \$5,000 pe	er day and \$nn,000 per month. There	is no enforcement of eithe	r
\$5,000. The highest eDeposit du	ring the period was for \$17,604,08.	2013 there were <u>nnnn</u> total deposits o Management should determine if enfo in excess of policy. Rating: Medium	r which nnn eDeposits exce proement of policies is expe	ected
Observation: The audit revealed	some confusion between various pa	articipants in the <u>eDeposits</u> process re ted amount were not possible. Manag	garding the limitation of de	posit
communication of actual practice	es to all parties involved.			
Finding: Mobile <u>eDeposits</u> is not not provide evidence of testing of Rating: Medium	currently a part of the Credit Union of their BCP. Management should en	's Business Continuity Plan. In additionsure that appropriate business continuity.	in, when queried, <u>Company</u> uity plans are in place and	B could tested.
Observation: Multiple departme	ents currently review transactions an	nd validate similar transactional attrib	utes. Management may wa	int to
	reviews currently performed are wa	arranted. ction volume or capacity therefore it is	impossible for the Credit L	Jnion to
				AST-C
TrustCC. All Rights Reserved.				
		1		
	Questions	and Answers?		