Time To Get Serious About Information Security
Disclaimer

This presentation is made available with the approval and authorization of the American Institute of Certified Accountants for this seminar.
Kim Chatani, CPA, CFE, CGMA, CFCA

- Advisory Partner at Khronicle Partners, Inc
- Board of Director and Audit Committee Chair at Far East National Bank, N.A.
- Adjunct Professor for School of Business at Concordia University, Irvine
- Accounting Instructor for the Department of Continuing Education for University of California, Irvine
- Former Audit and Consulting Partner for Arthur Andersen, KPMG Consulting and AT Kearney, Inc.
- Strategic business and technology advisor to MNCs w/30+ years of experience

chatani@khronicle.com
www.khronicle.com
What is Information Security Management?

- A systematic approach to encompassing people, processes and IT systems that safeguards critical systems and information, protecting them from internal and external threats.

Source: AICPA IT Membership Section
INFORMATION SECURITY CHALLENGES
Information Security Challenges

- Information moving to digital format
- Digital information knows no borders
- Information needs to be secured
- Physical security isn’t enough
- Info security requires legal & technical expertise
- Information security is a relatively new frontier
Primary Threats to Information

- Viruses
- Unauthorized access
- Theft
- Physical destruction
- Unintentional distribution
- Internal staff
DEFENSE IN DEPTH STRATEGY
Defense In Depth
STEPS TO SECURING YOUR SYSTEM
Improve Your Information Security

1. Data Protection
2. Malware Protection
3. Password Management
4. Mobile Device Protection
5. Wireless Security
6. Internet Security
DATA PROTECTION
Data Protection

Where is your data?
Protect Your Data

➢ Physical Security
  - Keys are used to secure assets
  - Assets are secured to protect the contents
    ▶ House key = secures the home
    ▶ Home is secured = protect contents and family

➢ Digital Security
  - Password are used to secure devices
  - Devices are secured to protect DATA!!
  - Accomplished via Encryption
Things to Know About Encryption

- Every privacy regulation requires it
- Loss of control of encrypted data does not constitute a breach of privacy
- Data should be encrypted when it is stored and in transit
- Some encryption tools are really simple and some are complex
- Think of encryption as a key to a lock
Encryption Example

Unencrypted File

Encrypted File

http://www
MS Office Encryption
Secure USB Drives
Guidelines for Protecting your Data

- Store data where you are directed
- DO NOT make unnecessary copies of sensitive data
- Treat data in your custody with due diligence
- Be mindful when disposing of data
- Encrypt sensitive data
- Use secure USB drives
- Destroy old USB drives
STORING DATA IN THE CLOUD
Cloud Storage Considerations

- Easy to Setup
- Free to Users
- Convenient Storage Location
- Enterprise Editions
- Mix of Security Configurations
- Backup of Your Data
Cloud Storage Services

www.box.com

https://onedrive.live.com

www.dropbox.com

https://drive.google.com
Guidelines for Using Cloud Storage

- Determine approved systems and communicate
- Use only services that encrypt In Transit AND In Storage
- Sensitive documents should be encrypted BEFORE storing
- DO NOT share sensitive files via a link unless encrypted
- Require user login when sharing files
MALWARE PROTECTION
Types of Malware

- Worms
- Spyware
- Ransomware
- Crimeware
- Trojans
- Phishing
- Viruses
- Adware

Malware
Effects of Malware

- Display Message
- Delete Data
- Disable Hardware
- Steal Data
- Corrupt Data
- Hijack Computer
- Slow Down Hardware
How Do You Get Malware?

Malware

- Click on Something
- Open a File
- Install Software
- Email Attachment
- Email Link
- Social Engineering
- Browser Search Hijacked
Social Engineering and Malware

- Attackers are Turning to Social Engineering to Bypass Anti-Virus Software
- Hacking people, not hacking technology
- Severity and impact on the rise
- Increased levels of deception
- Creative ways to get user credentials
- Creative ways to get information
Social Engineering Example

Voicemail from (202) 754-8391

"You or your criminal attorney. Call me back on my call back number because there is a legal case has been filed against your name for tax invasion for tax fraud so before this matter goes to federal claims court house or before you got arrested. Kindly call us back on number callback number. You got more details. The number you can reach me is 202754839182027548391. Again this is officer Richard Williams calling you from the Internal Revenue Service. Thank you."
Social Engineering Email Example

-----Original Message-----
From: Administrator [mailto:Administrator@Outlook-us.com]
Sent: Monday, January 30, 2013 10:14 AM
To: Janet Colligan
Subject: Important - New Outlook Settings

Please carefully read the downloaded instructions before updating settings.

http://damisillae.com/nulook/settings.html

This e-mail and/or any attachment(s) is intended solely for the above-mentioned recipient(s) and it may contain confidential or privileged information. If you have received it in error, please notify us immediately at helpdesk@Outlook-us.com and delete the e-mail. You must not copy it, distribute it, disclose it or take any action in reliance on it.
Social Engineering Phishing

NEW! Card Security Guarding Procedures

Valued CardMember,

This message is to inform you that All American Express(R) Card(s) now has new secure guarding procedures.

We have changed security guarding procedures for your American Express(R) Card(s). Please follow the given instructions in order to comply with our recent additional security features.

To continue, We have sent you an attached HTML Web Page.

- See e-mail attachment
- Download and save it
- Open the attached document
- Get started by filling your informations

Thank you for your continued Cardmembership.

Sincerely,
American Express Customer Service
Other Examples of Email Scams

- “We suspect an unauthorized transaction on your account, click here to login”
- “Your family member is stranded in Nigeria, send money…”
- “You have a secret admirer, click here to see their message”
- “You have a payment of $500 waiting in your PayPal account, click here to claim”
- “Click here to update your anti-virus software”
- “Click here to see an exclusive video of Robin Williams saying goodbye through his cell phone”
Ways to Avoid Malware

- Can’t Eliminate, Just Minimize
- Anti-Virus Software
- Browsing Protection
- Firewall Hardware & Software
- Windows Updates
- Knowledge, Awareness, Judgement
PASSWORD MANAGEMENT
The Connected World

Every site / app wants login

Logins available across platforms

Users have 100’s of logins

Can’t remember ID’s & passwords

Many write them down

Many make them the same
What is a Good Password?

- Unique, not re-used
- Min 8 characters
- Change every 90 days
- Caps, numbers, symbols
- Unknown to others
- Not written down
- Random, mnemonic
- Not in Dictionary
Password Management Using Password Keepers

- Saves your passwords in an encrypted file
- One “Master” password to decrypt the file
- Cloud-based to synch passwords across devices
- Fills in login screens for you
- Store other sensitive information like account & credit card numbers
What can Password Managers Keep?

- Mail account details
- Online identities
- Social networks
- Financial records
- Credit card data
- Health care data
- Web application passwords
- Social security number
Password Keepers

1Password

RoboForm
dashlane

LastPass
Security Tips for Password Managers

- Complex Master Password
- Don’t use Master Password for ANY other account
- Password reminders that no one else knows or can Google
- Use a Password Manager that doesn’t store Master Password on their system
- Implement Password Manager’s 2-Factor Authentication
2-Factor Authentication

- Multi-Factor Authentication
  - What you **know** (password, PIN)
  - What you **have** (token, card, chip, phone)
  - Who you **are** (fingerprint, iris, face)

- Password authentication = **Single-Factor** Authentication

- Two-Factor Authentication requires 2 of the 3

- Various ways to implement
How 2-Factor Authentication Works

- Create an account
- Provide information (email, phone #, fax #)
- Logon to new device or new location
- System knows this is new, so they send a verification code (via email, phone, fax, voice)
- Must enter verification code on new device/location
- 2nd factor is what you have
MOBILE DEVICE PROTECTION
How to Protect Your Mobile Device

- Find My Device
- Restrictions / Privacy Settings
- Location Tracking
- Backup
- Passcodes
- Data Protection
Passcodes / Lock Screen

- Must Enter to Access Device
- PIN, Swipe, Password, Biometrics
  - Caution: PIN & Swipe action left on screen
  - Password & Biometrics most secure
- Set to Immediate
- Screen Timeout
- Can be Policy Based
Location Tracking

- Tracks where you/device is or has been
- Allows apps to provide location based info
- Needed for Find My Device apps
- Allows mapping to provide route & traffic info
- iOS allows user to change per app
- A convenience feature
- Can be used for malicious behavior
What Does This Mean to You?

Just about anything you do & anywhere you go can be tracked.
Find My Device

- Find if lost or stolen
- Play sound to find
- Provide a message if stolen
- Lock the device
- Reset / Erase the device
- Available for both Android and iOS
Backup

- Ability to restore device & data
- Automatic vs. Manual
- Cloud vs. Local
- Data vs. Synced Content vs. Settings
- iOS provides complete Restore
- Android limited Restore
Data Protection

- Personal vs. Business Data
- Encryption
  - Slows device
  - Can’t be undone
  - Authorities can’t access without warrant
- Is Passcode enough?
- Sync with Cloud means 2 places for data
- Device memory vs. SD card
What is Wireless?

Any communications “over-the-air”
- Wi-Fi
- Cellular
- Bluetooth

Wi-Fi used to connect to network resources
- 100-200 feet

Cellular used to connect to internet using cellular data
- 2-3 miles

Bluetooth used to connect to accessories
- 30 feet
Wired vs. Wireless
Wireless Security

User ID: JohnDoe
PW: SuperSecret

Credit Card #, CID

"Plain Text"
<table>
<thead>
<tr>
<th>Wireless Encryption</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Open, unencrypted, weak security</td>
</tr>
<tr>
<td>WEP</td>
<td>Better than nothing, but very weak security</td>
</tr>
<tr>
<td><strong>WPA or WPA2</strong></td>
<td>Best encryption commercially available today</td>
</tr>
</tbody>
</table>
Wireless Security

User ID: #H*!&A*)
PW: *!@NS&%
Public Wi-Fi

- Must require PW to use Encryption
- All users are given the same PW
  - Easier
  - Too hard to give each user a PW
- Less support if provide open “hotspot”
- Risks
  - Malicious Access Points (attackers hotspot)
  - Spoofing Attack (send you to bad site)
  - Evil Twin Attack (fake hotspot)
Is a Wi-Fi Secure?

Indicates Unsecure connection
Guidelines for Securely Using Public Wi-Fi

- Impossible for establishment to completely secure
- Connect to PW protected Wi-Fi when available
- Confirm legitimacy of hotspot
- Enable firewall software
- Turn off sharing
Guidelines for Securely Using Open (Un-Secure) Public Wi-Fi

- Only use to browse websites that do not require login credentials
- Never install software when using public Wi-Fi
- Use only HTTPS (secure) websites
  - Logoff when done
- Use a VPN software (Review or PCMag)
- Forget Wi-Fi before leaving area
Enable Firewall Software
Turn Off Sharing

**Advanced sharing settings**

**Change sharing options for different network profiles**

Windows creates a separate network profile for each network you use. You can choose specific options for each profile.

- **Private (current profile)**
  - [ ] Turn on network discovery
  - [ ] Turn off network discovery

- **Guest or Public**
  - [x] Turn off network discovery

**Network discovery**

When network discovery is on, this computer can see other network computers and devices and is visible to other network computers.

**File and printer sharing**

When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.

- [ ] Turn on file and printer sharing
- [ ] Turn off file and printer sharing

**All Networks**

[ ]
Forget Wi-Fi Access Point – Windows 8.1

Open the Charm Bar > Settings > Networks > Right-Click Wi-Fi

- Show estimated data usage
- Set as metered connection
- Forget this network

Connect automatically
Browse the Web Safely

:::pullquote

**Reported Attack Page!**

This web page has been reported as an attack page and has been blocked based on your security preferences.

Attack pages try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack pages intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.
URL Structure

http://www.companyname.com/folder/index.htm

- Protocol
- Registered Name
- TLD (Top-Level Domain)

HTTP "cleartext"
Trusted Sites

- Ordinary Site:

- Trusted Site — **Note:** Green Background on URL line
HTTPS

HTTPS, no Green Background, but Lock

Select Login Green Background and Lock
HTTPS “Lock” (Certificate)

Click on the “Lock” to view info about the Certificate

Certificate Authority validates identity of the website

Click on the View Certificates for details
HTTPS Certificate Warning

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

- Click here to close this webpage.
- Continue to this website (not recommended).
- More information
  - If you arrived at this page by clicking a link, check the website address in the address bar to be sure that it is the address you were expecting.
  - When going to a website with an address such as https://example.com, try adding the 'www' to the address, https://www.example.com.

For more information, see "Certificate Error" in Internet Explorer Help.

When there is an issue with the Certificate, you will get this warning!!
Untrusted HTTPS Certificate

URL background is RED

Click "Shield" for details

A certificate must have 3 items to be valid:
1) Issued to the website
2) Issued by a Trusted Authority
3) Not expired
Look Before You Click

Click a “Link” on a webpage will display the URL in the Status Bar of most browsers.

Click a “Link” in an email will display the URL above the cursor.
Guidelines for Browsing the Web Safely

- Use a current, updated, trusted web browser
  - Internet Explorer, Chrome, Safari, Firefox
- Avoid installing unnecessary add-ins, plug-ins, or toolbars
- Use secure websites (HTTPS)
- Pay attention to the TLDs (Top-Level Domain) and registered names for web content
- Verify the targets of links
CONCLUSION
Thank You!!

Kim Chatani, CPA CFE, CGMA, CFSA
chatani@khronicle.com

Khronicle Partners, Inc.