CYBERSECURITY – PLEASE, NOT AGAIN!

A Conversation with the County Treasurer
September, 29, 2017
Who am I? and What do I do?

- Joseph Kelly
- Los Angeles County Treasurer and Tax Collector, *ex officio*, Public Administrator
- I report to the five member Los Angeles County Board of Supervisors
- I am appointed by my Board; I am not elected

<table>
<thead>
<tr>
<th>TREASURER</th>
<th>TAX COLLECTOR</th>
<th>PUBLIC ADMINISTRATOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Safekeep all the money</td>
<td>• Bill and Collect Secured and Unsecured Property Taxes</td>
<td>• Perform estate administration services for those persons who die in the County and do not have any known heirs</td>
</tr>
<tr>
<td>• Manage all bank relationships</td>
<td>• De facto Business License Issuer</td>
<td></td>
</tr>
<tr>
<td>• Process all remittances</td>
<td>• Miscellaneous taxes (UUT and TOT)</td>
<td></td>
</tr>
<tr>
<td>• Issue all debt</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Manage credit rating agency relationships</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Presented at Los Angeles County Office of Education September 29, 2017
Let’s start with definitions

- Cybersecurity is the sum of efforts put forth to manage cyber risk.

- Cyber risk is the exposure of an organization to harm or loss resulting from breaches or attacks on the organization’s information technology infrastructure.
Cyber Risk Analysis: Online Payments

- Online payments of secured property taxes surpassed $1 billion in first installment 2014-2015

- All sorts of risks accrue if a breach occurred
  - Costs increase as taxpayers could revert to paper checks
  - Customer service demands increase
  - Compromises strategic downsizing in remittance processing infrastructure
  - Lose efficiencies built into online processes and automated refund processes

- Conclusion: perform a cybersecurity assessment of eCommerce payment module
Cybersecurity assessment

- Constituted an ad hoc work group of the County’s Risk Manager, Chief Information Officer, and Director Internal Services Department

- Determined scope of assessment, notified my Board, and applied for, and was awarded, a matching grant from the County’s Quality and Productivity Commission (no centralized funding)

- This was to be the first ever, pro-active cybersecurity assessment conducted in a County department

- The Chair of the Quality and Productivity Commissioned noted in his annual message that “A visionary Treasurer-Tax Collector took a pro-active approach to cybersecurity.”

- Assessment identified a number of findings, none of which compromised the security of the transaction. Implemented all corrective actions.
Why is this here?
I was “whaled”

- Phishing emails go to a wide group of people without targeting anyone.
- Whaling are phishing attempts targeted at the big guy or gal, the Whale!
- I received an email from a recognized financial partner regarding an overdue invoice. When I opened the overdue invoice, I noticed a “.de” extension when my mouse was hovering.
- The next day my secretary interrupted a meeting and passed me a note which said “The Police are here to see you.”
- Conducted risk assessment post event. Challenges of managing in the public sector given our public records.
Where is my FedEx package?

- How a simple inquiry led to the following:

This is to inform you that this morning my IT staff determined a ransomware virus had infected a limited portion of the Department’s computer network. A ransomware virus takes hold by encrypting files and a user is not able to access the files until the user obtains a password required for decryption. The user typically obtains the password by paying the originator of the ransomware a required “ransom.”

Since late yesterday afternoon when my staff first identified the suspicious activity, we implemented a number of investigative and preventative protocols that allowed us to not only identify the staff computer from which the virus originated, but to quarantine a number of others. At the point that we received indication of ransomware, we engaged the District Attorney, in compliance with required protocols. The DA will work with my department and the Chief Information Office to investigate the matter. By working in conjunction with McAfee and restoring the previous day backups, my staff will be able to restore operations without payment of the "ransom."

A review of the ransomware and consideration of the actual “ransom” asked ($250) indicates this was a common, low level phishing attempt. At no point were the assets of the County Treasury compromised in any way.
Six months after I took this action, the County restricted access to personal email accounts from County workstations.
My day at the Citibank Cyber Security Fusion Center – very, very cool!

Photo is not of the actual CCSFC visited
Training is a critical component of every cybersecurity plan

- The County Risk Manager has established a series of online training courses, under the umbrella of a Risk Management University.
- The topic of cybersecurity should be a standing item on every staff agenda.
- Risk management protocols and practices in one business line may be different than those in others (e.g., FedWire system for money movement is not a hospital billing record.)
- Develop mechanisms to monitor staff compliance with cybersecurity directives (e.g., centralized issuance of phishing emails, with centralized reports of staff who clicked on links they should not have.)
- Evaluate staff non-compliance from a performance management perspective.
Wrap up and conclusions

■ Cyber risk rules. Manage it and manage it aggressively.

■ Step outside your comfort zones. Don’t be afraid to set precedent.

■ Train smart – simplify the messaging. See following slide.

■ Engage staff at the Unit level in discussions about the importance of protocols and procedures.

■ Monitor staff compliance.
Do you protect your cyber sphere the same way you protect your home?
Cyber cidebar (1 of 2)

■ Password management
  ➢ Use really strong passwords (30+ characters if permissible) and change them every 30 days.
  ➢ Develop a theme for the password: old TV shows you love (IMissLoveBoat%79Alot) or movie stars you wanted to date (IfOnlyIHadDatedHarrison#321Ford)

■ Limit what you share
  ➢ Not everyone needs to know that you away from the office, so why tell them? Turn off “signature” lines in your cell phones informing everyone that you sent that email from a mobile device. Establish consistent fonts/sizes across all devices.
  ➢ Instruct support staff not to discuss your schedule and limit access to your calendar.
  ➢ Limit your published biography. Do you know from this presentation that I have a Ph.D.?

■ Limit ability for someone to spy on you and/or your physical space
  ➢ Put tape over all cameras connected to workstations or laptops so that in the event someone does hack in, they can’t also spy on you. Turn off camera functionality in cell phones.

■ Own your brand, so no one else can
  ➢ I registered jkelly@ttc.lacounty.gov at LinkedIn so no one else could.
Cyber sidebar (2 of 2)

- Your cell phone - if not managed correctly - is the equivalent of giving the keys to your house and the alarm codes to a robber.
  - Appreciate that Wi-Fi networks are not secure, so don’t use them.
  - Limit the ability of someone with a scanning device to attach your cell phone device to you. Name your cell phone device with a name that does not correspond to your name, your gender or ethnicity. Example: Joe Kelly’s IPhone is replaced with Sofia Ramirez IPhone. If someone scans a room in which I am in for my device, they won’t find it.
  - Turn off Wi-Fi on your cell phones and laptops at the same time you would turn the sound to off/vibrate. Begin to link the two actions together (sound to off/vibrate and Wi-Fi to off.)
- Disconnect all home Wi-Fi networks as frequently as you can, but certainly before a weekend get away and vacation.
- Do not conduct work business on non work devices.