# CYBERSECURITY FRAUD: HOW TO ADDRESS RISK IN TODAY'S MARKETPLACE

Presented by: Michael Cretaro, Consultant ACC Technical Services

## RISKS

- Improper IT maintenance/aging infrastructure
- Understanding cybersecurity vulnerabilities
- Lack of cybersecurity policy
- Confusing compliance with cybersecurity
- The human factor people are the weakest link
- BYOD & the cloud
- Resource constraints
- Inadequate or non-existent business continuity & incident response plans
- Corporate inflexibility
- Accountability



#### RANSOMWARE

LARGEST CURRENT THREAT



#### WHAT IS RANSOMWARE?

"Ransomware is a type of malicious software from cryptovirology that blocks access to the victim's data or threatens to publish it until a <u>ransom</u> is paid." -Wikipedia

A giant pain in the keister!

-Mike Cretaro



- Email
- Unpatched software
- Thumb drives
- Websites
- Viruses
- Rerouted internet traffic
- SMS (text messaging)



• Email

	From: First Generic Bank <accounts@firstgenericbank.com> Subject: Please update your account information Date: Sep 12, 2006 3:23 PM PST</accounts@firstgenericbank.com>	
Generic greeting	Dea⊳First Generic Bank user,	
	As a courtesy to our valued customers, First Generic Bank conducts regular account information verification processes. During the most recent process, we found that we could not verify your information.	
No "https"	In order to ensure your account information is not made vulnerable, please visiphttp://www.firstgenericbank.com.account-updateinfo.com.	Forged link
Requests personal info	Please click on the above link to our Web site and confirm or update your account information. If you do not do this within 48 hours receipt of this e-mail, you will not be able to use your First Generic Bank account for 30 days. This is an extra precaution we take to ensure your account remains secure.	Sense of urgency
Generic sender	Sincerely,	
Generic Sender	► First Generic Bank	

Technical Services





Unpatched software

• IOT – the Internet Of Things









• Thumb drives









• Websites

• Rerouted internet traffic

Major sites including New York Times and BBC hit by 'ransomware' malvertising

Adverts hijacked by malicious campaign that demands payment in bitcoin to unlock user computers

#### Home Routers Being Targeted in DNS Hijacking Attack, Trend Micro Says

Attackers attempting to steal sensitive data by diverting home router traffic to malicious domains, security firm says.

Technical Services

• Viruses





#### SMS (text messaging)

••• Network 4G	8:40	õ∦ 97% <b>■●</b>
K Messages	+0312345678	9 Contact

Text Message Today 06:51

Dear OCBC Bank User, We have detected some unusual activity. We urgently ask you to follow the account review link: http://bit.do/ocbc-bank

4:21 PM	* 22% 💭
iCloud	Details
	4:21 PM iCloud

iCloud: Your ID requires verification: <u>www.id-apple.mobi</u>

\* 🗸 📔 14:08 Ŧ App info Q PERMISSIONS This app can access the following on your phone: **L** read phone status and identity edit your text messages (SMS or MMS) read your text messages (SMS or MMS) receive text messages (SMS) receive text messages (WAP) send SMS messages this may cost you money read your contacts modify or delete the contents of your ŵ USB storage read the contents of your USB storage **1** full network access view network connections view Wi-Fi connections 0  $\triangleleft$ 

**Technical Services** 

# Stolen credit card numbers worth a few dollars

#### TARGETS

- People are the #1 target
- Unpatched software
- Companies with valuable data
  - PII Personally Identifiable Information
  - PHI Protected Health Information
  - PCI Payment Card Industry (credit card data)
  - Anyone with money

Stolen health records worth \$350-\$500 each



#### WHAT DOES IT DO?

- From the infected machine, it accesses every file it can
- Encrypts the data with strong encryption keys
- Exfiltrates the data for possible use later
- Deletes backups if accessible
- Notifies the user of the "ransom"
- Installs backdoors for possible later "re-infection"



# HOW DO WE RECOVER?

- Should we pay the ransom?
  - There is no guarantee they will decrypt your files
  - Strong possibility they've stolen the data even if you pay
  - If you have good backups, then restore from backup
- Erase all affected systems and start over
  - Servers if this was the point of infection wipe and reload – can be time consuming
  - Workstations erase and apply standard image reinstall necessary applications
  - Share drives delete share and restore from backups



# Security Is Uncomfortable

#### HOW DO WE PROTECT?

- Cybersecurity policy including incident response
- Employee training
- Anti-virus & anti-malware software (only the start)
- DNS monitoring
- Backups: onsite and offsite
- Strong password policies
- Principle of Least Privilege
- LEM/SIEM threat monitoring
- Cybersecurity insurance
- Pen test



# QUESTIONS?



# CONTACT:

Michael Cretaro

Office: 315-484-4500

Cell: 315-952-6473

Email: mcretaro@acctek.com

