2019 Annual Seminar

Presentations Available at www.tmrs.com/ats.php
Member Services and Security

Wrangling Security Threats

Eric Obermier, Assistant Director of Information Resources
Oscar Guzman, Information Security Analyst
Debbie Muñoz, Director of Member Services
Moderator: Sandra Vice, Director of Internal Audit
Topics of Presentation

• Why online security matters
• Mitigating threats through best practices
• What TMRS is doing
• When “it” happens
• Resources
Recent Events – Cybercrime in the News

• Texas cyber incident affected 22 local entities
• Data breaches (throughout the year)
• Equifax finally settled
Audience Polling Question

1. Our city has been a victim of a ransomware attack.
   a) Yes
   b) No
   c) Don’t know
Cybercrime Statistics

• US and global cybercrime stats
  • 446 million consumer records with personal information were stolen by hackers in 2018
  • 60 million Americans were affected by identity theft in 2018
  • Less than 50% of companies globally are sufficiently prepared for a cyberattack
  • 350% growth in ransomware attacks annually, and damage costs will rise to $10 billion in 2019

• Escalation of cybercrime in public sector agencies
  • Government has been among the five most cyberattacked industries over the past five years
Why Does This Matter to You?

- Financial loss
- Data breach
- Compromised personal information
- System unavailability
- Reputational loss
- Recovery
- Time and effort
- Personal application
Terms and Concepts

- Phishing, Vishing, and Smishing
  - How to identify
  - How to defend
- Ransomware
- Password Security
  - Password managers

Estimated Ransomware Costs – Texas 2019

- County: $3,250,000
- City: $2,340,000
- Education: $1,800,000
- Unreported: $5,000,000

Source: Texas DIR and TAMU System
2. When creating a password, you should:

a) Use your family member name, sports name, pet name, and add a number at the end (Smith123)

b) Use phrases or misspelled words with numbers and special characters sprinkled in (w3hvAf@lur2comun!kt)

c) Use sequential letters and number from your keyboard (QWERTY1)
Internal Threats

- Bob – clicks on phishing emails
- Jan – circumvents security controls to watch movies (example)
- Dan – browses non-business related websites infected with malware
- Mary – plugs in a USB drive to see what’s on it
- Andy – lets service personnel in without supervision

95% of data breaches are attributed to human error.

Source: Cybint Solutions
What Is TMRS Doing?

Technology
• Multi-factor authentication
• Web fraud detection tools
• Caller verification

Headline from Forbes about a UK-based energy firm:
A Voice Deepfake Was Used To Scam A CEO Out Of $243,000
3. TMRS’ multifactor authentication may ask members to provide:

   a) Their Social Security number
   
   b) Their address
   
   c) Their phone number

Password + Verification = Access
What Is TMRS Doing? (continued)

Education and Culture

• Security Awareness Training
• Data privacy program
• Fraud Committee
Cybersecurity Best Practices (Email)

- Check the sender's name against the sender's address
- Ignore suspicious or unexpected links/attachments
- Hover over hyperlinks
- Use unique, strong passwords for all accounts (password manager)
- Do not provide personal or organizational information unless you are sure of the requestor's authority, identity, and legitimacy
Just Another Manic Monday....

• It’s Payroll Monday
• You’re running late
• You grab your coffee, take a seat at your desk, and turn your computer on....

AND “IT” HAPPENS
Congratulations... You’re Under Attack

Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don’t pay in 7 days, you won’t be able to recover your files forever. We will have free events for users who are so poor that they couldn’t pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am (UTC). Bitcoin Accepted Here.

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Contact Us

Payment will be raised on
5/18/2017 19:40:10
Time Left
01:20:04:50

Your files will be lost on
5/22/2017 19:40:10
Time Left
05:20:04:50
Actions When “It” Happens

• Alert your IT staff or supervisor
• Activate your incident response plan (yes, you need one!)
• Consider involving law enforcement
• Report to TMRS at 1-800-924-8677
4. My city’s IT resources are best described as follows:

a) We have our own internal IT staff.

b) We use an IT contractor (third party) for IT services.

c) None of the above. We are on our own.
Culture

• It’s safe to say something / safe to act
• Talk internally about security
• Empower employees to give feedback
  • Training
  • Security
  • Processes
  • Incidents
Cybersecurity Training – New Law
HB 3834, effective 6/14/19

• Annual training must be completed by June 14, 2020!

• Who? Local government entities’ employees and elected officials who have access to a local government computer system or database

• Texas Department of Information Resources (DIR) will certify cybersecurity training programs, or...

• Local governments with a dedicated cybersecurity officer can use their own cybersecurity training program
Resources

• Texas Department of Information Resources

• Cybersecurity Training & Exercises | Homeland Security
  https://www.dhs.gov/cisa/cybersecurity-training-exercises

• Free SANS resources (also recommend subscribing to their free OUCH! newsletter)
  https://www.sans.org/security-awareness-training/resources

• Some basic personal awareness/phishing tests
  https://www.opendns.com/phishing-quiz/
5. The first action I will take when I get back to the office is:
   a) Change my passwords to make them harder to guess.
   b) Ask for online security training.
   c) Find out if we have cyber insurance and a security incident plan.
Key Takeaways

• Be proactive
• Training is ongoing
• Be vigilant
• Report, report, report

Remember: Security is not a destination, it’s a journey!
Questions?

Presentations Available at www.tmrs.com/ats.php