FORTIUM
Partners

Government Finance Officers Association of Texas
Cyber Security Forum

November 15, 2019

Today’s Goals

- Review current cyber-crime landscape
- Explore readiness to identify, protect, detect, respond and recover
- Provide additional information to take with you

Cyber Attacks By the Numbers

- 170: Number of county, city and state governments attacked since 2013 (as of July 2019)

- 150-250: Average min/max number of days it takes to **detect** a cyber breach

- $75,000: Average ransomware payment; some payments in the millions

- 59: Percentage of ransomware attacks that originate with phishing emails

Cyber Attacks By the Numbers

- 50: Average number of days spent to remediate a cyber breach
- 22: Number of towns in Texas attacked in the **first half** of 2019
- 10: Cost of operational downtime multiplier compared to ransom requested
- 1: Estimated number of attacks reported to authorities for every 4 that occur

City Example 1 – June 2019

- Know what’s connected
  - Population: 3,300
  - Event: Ransomware
  - Actions taken: Unknown
  - Operational Impacts
    - City systems were encrypted, including associated phone lines which were rendered useless
    - Ransom requested 8 bitcoins worth about $40,000 at the time
    - Hackers provided directions for downloading an alternative browser and making ransom payment

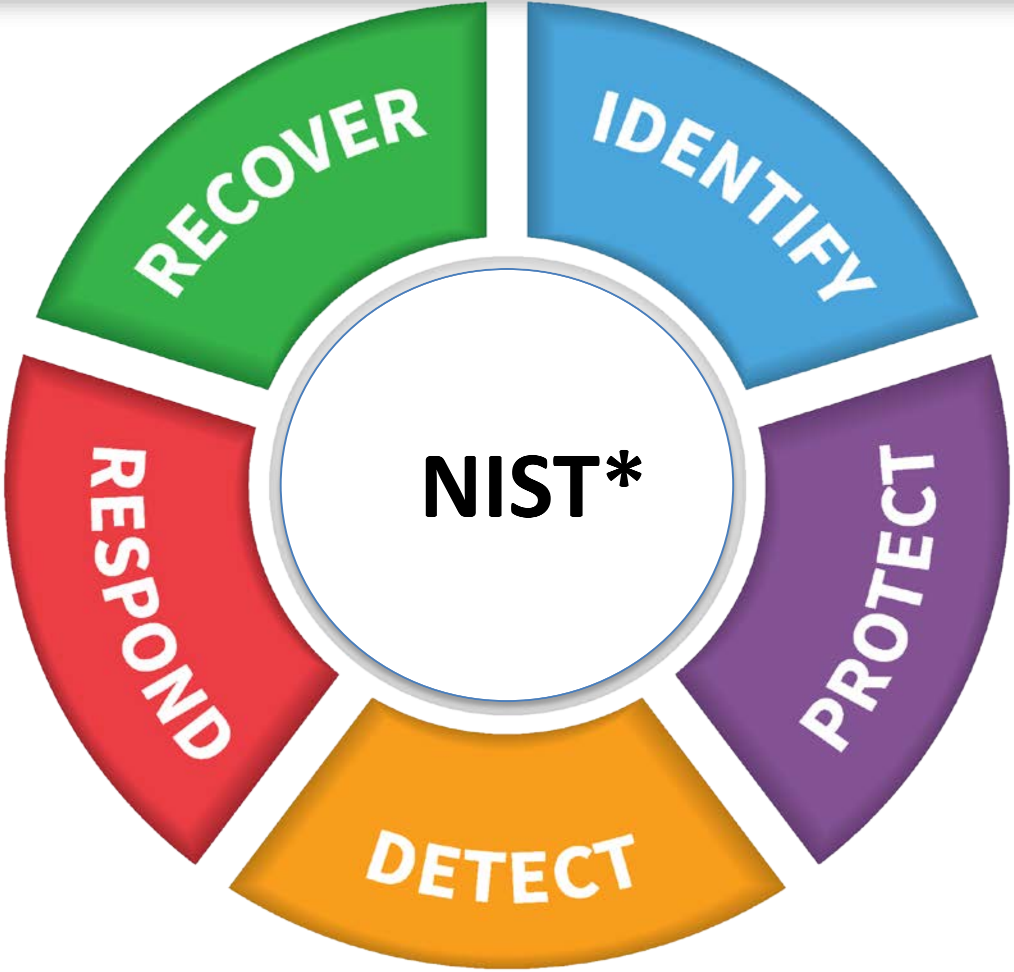
City Example 2 – May 2019

- No technology required
  - Population: 875,000
  - Event: Email phishing
  - Actions taken: Unknown
  - Operational Impacts
    - Hacker utilized scam email that appeared to be from city’s vendor
    - Email requested change to the bank account for electronic deposit
    - City lost nearly $700,000

Common Themes

- Cyber criminals target counties and cities of all sizes
- Cyber attacks most commonly come through email phishing and result in malware and/or ransomware
- Full extent and severity of impact may not be immediately evident and may be operational, financial and/or reputational
- Fall back operations often involve manual processing
- Employees and other system users, if properly educated, are a key line of defense against cyber criminals
- The appropriate security posture is not ‘if’ you will be attacked, but rather ‘when’ and ‘how will you respond’

Are You Ready?



* National Institute of Standards and Technology

Are You Ready?

NIST
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER

Identify

- ✓ Priorities and decision makers
- ✓ Everything: devices, data, networks
- ✓ Who ~~should~~ can access it?
- ✓ Classification?
- ✓ Connection?

FORTIUM Partners

Are You Ready?

NIST
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER

Protect and Detect

- ✓ Block unauthorized entry **and** activity?
- ✓ What “valuables” require special treatment?
- ✓ Avoid the credentials snowball
- ✓ How are you staying on top of patching?
- ✓ Will they know “something” when they see it?
- ✓ Starts slowly and under the radar….how will you know?

Are You Ready?

RECOVER
IDENTIFY
NIST
RESPOND
PROTECT
DETECT

Respond

- ✓ Who’s in charge?
- ✓ What’s the priority?
- ✓ Data loss (confidentiality, integrity, availability)?
- ✓ What operations and services keep going?
- ✓ Backups?
- ✓ What do we tell employees, citizens, constituents, leaders?
- ✓ Policy decisions?

Are You Ready?

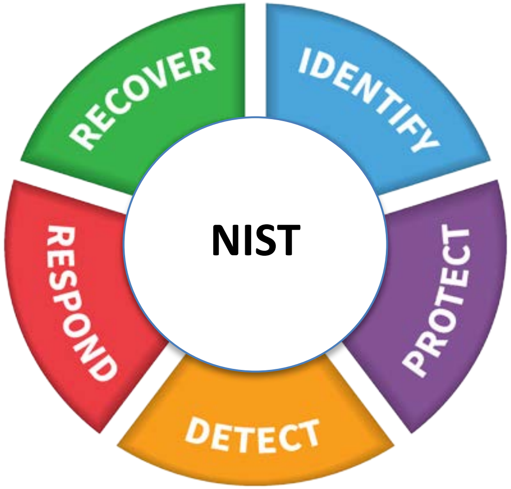
NIST
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER

Recover

- ✓ Who leads recovery?
- ✓ Order and timeline
- ✓ When were procedures last tested?
- ✓ We’ll know recovery is complete when….?
- ✓ Communication: who, when, how often?
- ✓ After-action review and post-recovery improvements?

Resources To Get Discussions Started

Security Vocabulary



NIST Sample Questions

Good Cyber Hygiene Checklist

Where to Go From Here?

Use the NIST Framework to Ask Readiness Questions

- Document your assets, critical data, key personnel, and core business processes before addressing technology details
- Use the questioning process to reveal risks and priorities
- Be intentional about classifying and securing data (Public, Sensitive, Confidential, Regulated)
- Recognize that “we don’t know” or “we don’t have” answers will help drive remediation actions
- Drive decisions that require agreement among key business and technology leaders

Where to Go From Here?

Evaluate the Answers Before Solving the Problem

- Answers will point out highest security needs and appropriate responses
- Answers will drive both business and technology decisions to combat and respond to cybersecurity attacks
- Answers will provide the basis for making cybersecurity product and/or service decisions
- Answers will help prepare for today's threats, as well as for what tomorrow might bring

What Help Might I Need?

Engage a strategic partner with cybersecurity expertise

- Provide a facilitated, expert-driven process of asking the questions and evaluating the answers
- Develop a prioritized remediation plan and help manage execution
- Guide identification, selection and management of cybersecurity products and/or providers based on prior experience
- Create a plan for ongoing security assessments and remediations to combat future threats
- Guide incident response and remediation

How Fortium Can Help

- ✓ Provide an assessment
  - ❖ Security
  - ❖ Best practices
  - ❖ Technology staffing
  - ❖ User needs & wants
- ✓ Technology Leadership as a Service (TLAAS)
  - ❖ Strategic planning
  - ❖ Application selection
  - ❖ Implementation project management
- ✓ Be an objective leader for tactical and strategic action aligned to your risk profile and other identified needs
- ✓ Provide desired scope to drive operations and results