



Best Practices in Cybersecurity



To partner with local governments so that Texas communities are

STRONGER TOGETHER



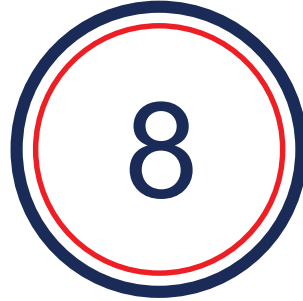
It won't happen to us

**Ransomware Attack Will Cost Baltimore Over
\$18 Million**

**Alarm in Texas as 23 towns hit by
'coordinated' ransomware attack**

Cost of City of
Atlanta's cyber
attack: \$2.7 million —
and rising

*'Dangerous Stuff': Hackers Tried to Poison
Water Supply of Florida Town*



Best Practices

1. Backup data
2. Third - party vendor management
3. Cyber insurance
4. Incident Response Plan
5. Multi - factor authentication
6. Train employees
7. Institute principle of least privilege
8. Establish policies



Data Backups

- ◆ Easy as 3, 2, 1...
- ◆ Disaster recovery and application availability
- ◆ Test your backups
- ◆ Know your Recovery Point Objective and Recovery Time Objective
- ◆ Encrypt and physically protect



Third - Party Vendor Management

- ◆ Contract management
- ◆ Scrutinize vendor's security and validate
- ◆ Know the who, what, when, where, and how
- ◆ Vendor inventory – and track it



Cyber Insurance

- ◆ Know the Terms & Conditions
- ◆ Panel of providers?
 - ◆ If not, what are the requirements?
 - ◆ Pre-breach vs. post-breach
- ◆ What are the requirements for renewal?
- ◆ Don't rely on cyber insurance alone



◆ Cybe

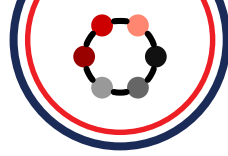


lan



Create an Incident Response Plan

- ❖ Cyber event is a DISASTER
- ❖ Identify business needs (systems and processes)
- ❖ Clearly defined roles and responsibilities....written down
- ❖ Top-down support, all departments engaged
- ❖ PRACTICE!!



Implement MFA

- ◆ Remote access
- ◆ Privileged user accounts?
- ◆ External facing applications
- ◆ Enable on Office 365
- ◆ Cyber insurance?



Train Employees

- ◆ Overall cyber awareness
- ◆ Physical device security, physical premises security, public WiFi, USB
- ◆ Simulated phishing campaigns



Institute PoLP

- ◆ Minimum access necessary for job duty
- ◆ Software installation/updates/patches all handled by admins
- ◆ Unique and distinct admin accounts for each set of admin tasks
- ◆ Create non - privileged accounts for all non - privileged tasks



Establish Policies

- ◆ BYOD, Acceptable Use, Information Security, Social Media Use, Remote Work
- ◆ Passwords (20 characters?)
- ◆ Onboarding and Separation
- ◆ Wire Transfer



A Few last Thoughts...

- ◆ Cybersecurity is Risk Management
- ◆ People, Processes, Technology
- ◆ If you detect an incident:
 - ◆ Immediately isolate affected system (keep machine running)
 - ◆ Secure backups (offline, secure, scan)
 - ◆ Collect/ review logs
 - ◆ Solicit assistance from third-party experts/ notify cyber carrier
 - ◆ Report incident to CISA and/ or FBI
- ◆ We must be perfect, all the time. Hackers just have to be right ONCE.



Any questions?

You can find me at:

rburns@tmlirp.org · 512.491.3427

Ryan Burns, Cyber Risk Services Manager