TML
INTERGOVERNMENTAL RISK POOL

The Cybersecurity Pandemic:

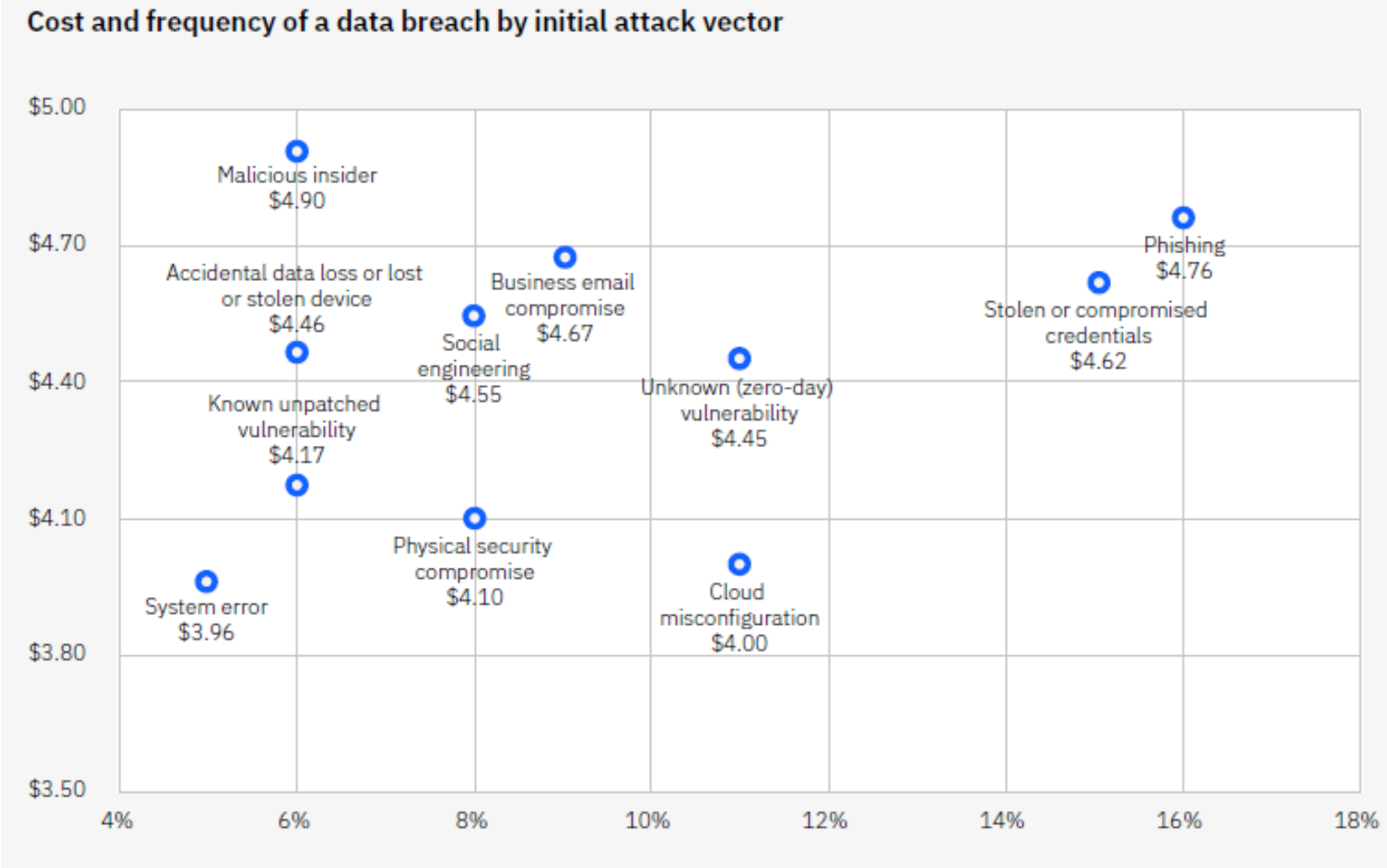
Essential Best Practices for Today's Threat Landscape

To partner with local governments so that Texas communities are STRONGER TOGETHER

Claims – What are Our Members Seeing

- Fraudulent Instruction/EFT
  - BEC on Member's side
  - BEC on Vendor side
- Ransomware
  - Encryption of Data
  - Double Extortion
- Supply Chain
  - IT vendor
  - Service Provider

What do 90% of these claims have in common?



** Measured in USD millions, per IBM Security: Cost of a Data Breach Report, 2023*

3 Pillars of Cyber Security

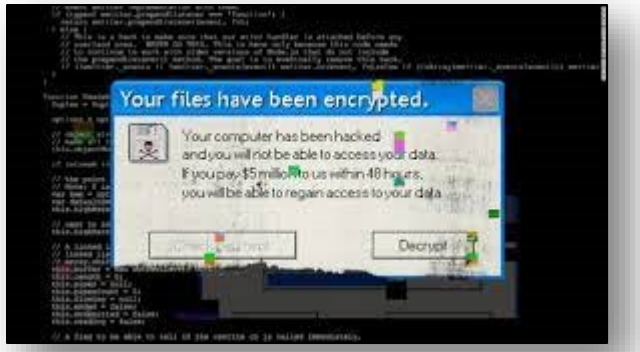
Where Should I Focus My Resources

1. Backup data
2. 3rd party vendor management
3. Cyber insurance
4. Advanced endpoint protection
5. Patch often
6. MFA
7. Train employees
8. Institute PoLP
9. Establish policies
10. Incident Response Plan

A Cyber Event Is a DISASTER

Disasters come in many forms:

- Tornadoes
- Floods
- Hurricanes
- Earthquakes
- Fires
- Utility outages
- Active shooter/mass casualty events
- Cyber attack/data disaster



Incident Response Plan

Incident Response Planning

Business Impact Analysis

Business Continuity Planning

Cyber Incident Response Plan

Business Impact Analysis

- Identify critical business functions
- Determine dependencies
- Assessing impact
- Setting Recovery Time Objectives (RTO)
- Identify resource requirements
- Risk Assessment
- Document results
- Recommendations and mitigation strategies (Business Continuity Plan)
- Periodic reviews and updates

Business Continuity Plan

Emergency response and crisis management	Business recovery and continuity strategies	Employee support and safety	Communication plan
Testing and training	Documentation and reporting	Governance and leadership	Legal and regulatory compliance

How Business Continuity and Disaster Recovery Relate

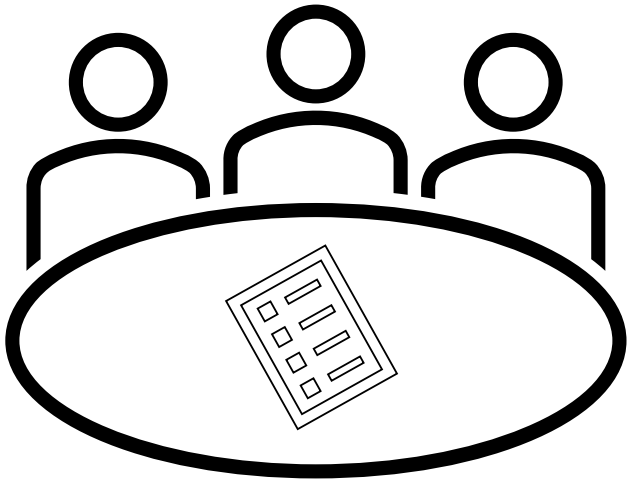
- Business Continuity
  - Encompasses a broad scope of the organization's functions.
  - Concerned with maintaining operations.
  - Does your organization have a list of critical functions?

- Disaster Recovery
  - A subset of business continuity planning.
  - Focused on recovery of IT infrastructure, systems, and data.
  - What IT systems support your organizations critical functions?

** Texas DIR*

Consider What Goes in Your Incident Response Plan

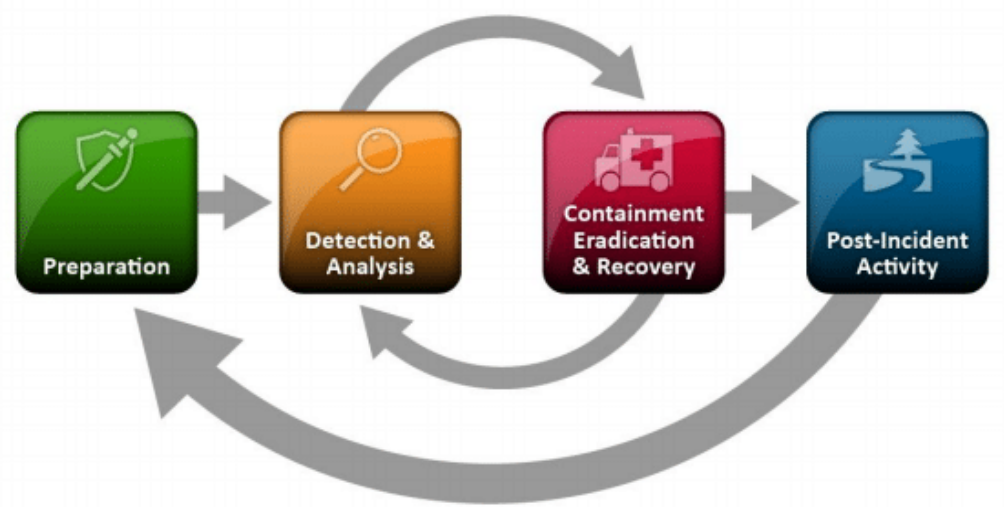
- Identify Your Team
  - Who will be on the incident response team? Will we have several team components?
- Decide Who Gets Notified and When
  - Who will be notified when we activate our incident response plan? Who makes those decisions?
- Document Your Environment
  - Do we have an inventory of our systems? Do we need to develop a network diagram?



** Texas DIR*

Begin Drafting Your Incident Response Plan

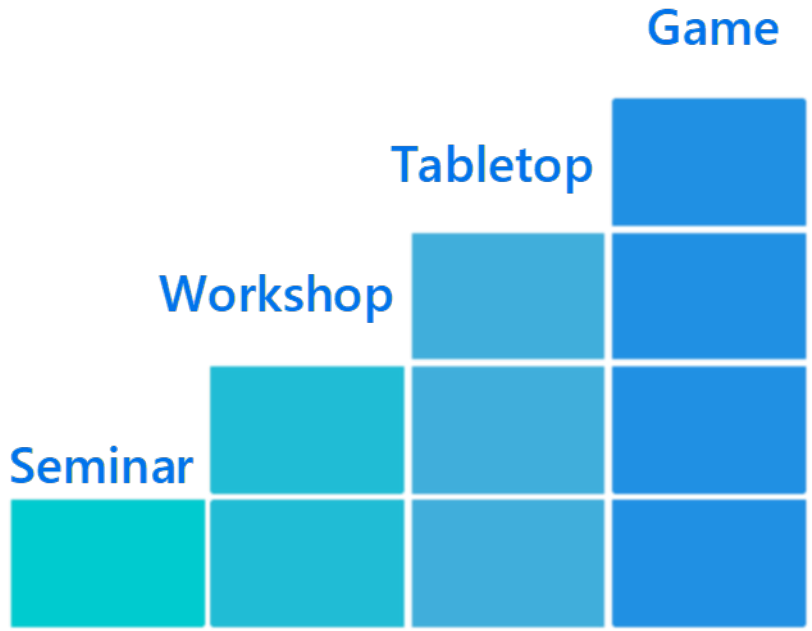
- Identify What Resources Can Assist You
  - What resources will assist with incident response? Will these resources be from inside or outside of the organization?
- Define Your Response Strategy
  - How will we contain an incident? What will we do to eradicate the threat so recovery can begin?



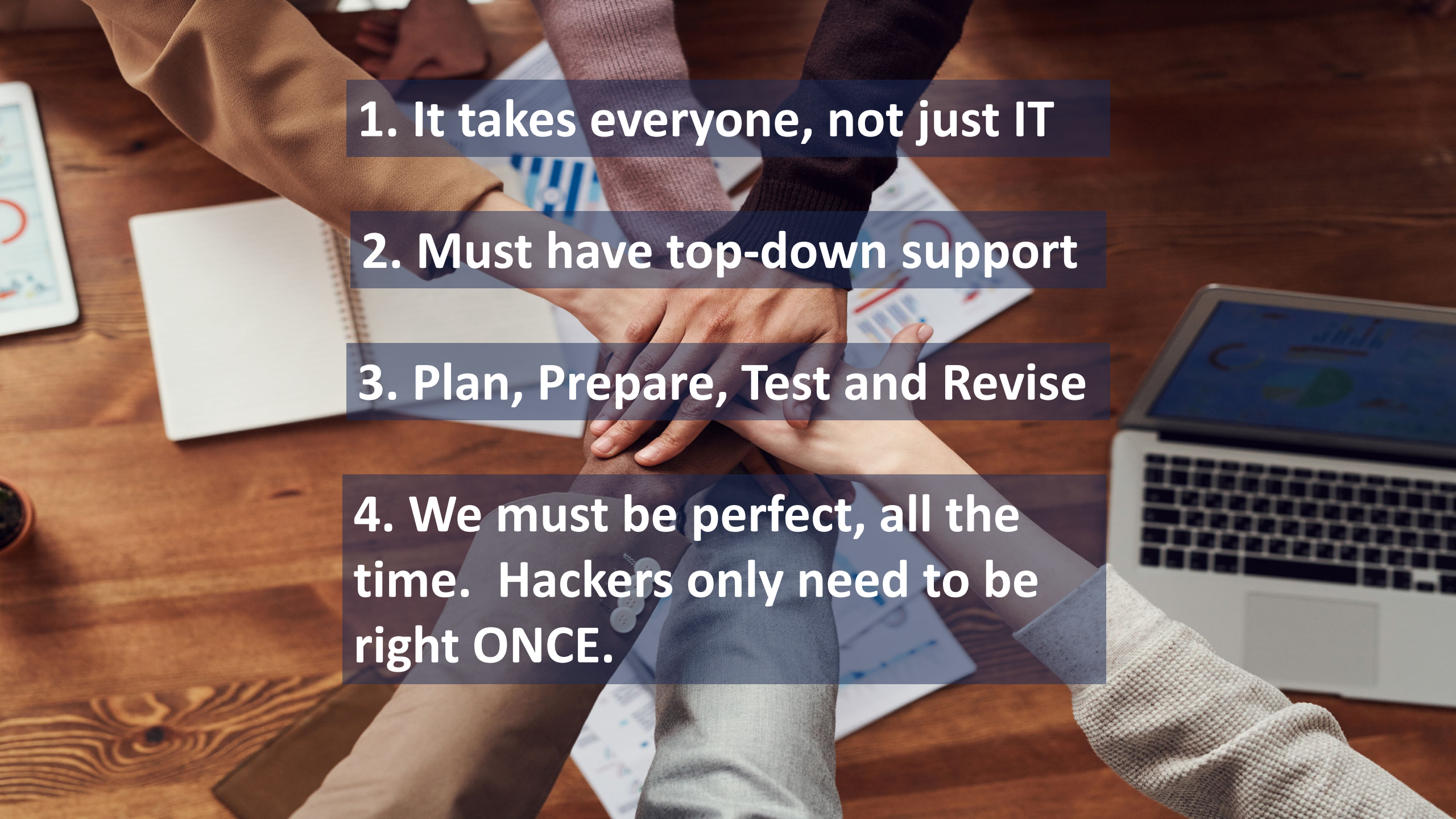
** Texas DIR*

Craft the Perfect Starter Exercise

- Select the Right Scenario
  - Begin with a simple scenario such as a lost device or phishing attempts. Is there a recent incident you could use as a scenario?
- Start Small
  - Limit initial participation to the core response team. Who do we want to participate in our inaugural exercise?
- Build Over Time
  - Add leadership as staff become more comfortable with the process. What does leadership want to exercise?
- Leverage Available Resources
  - Use pre-built tabletop resources to your advantage.



** Texas DIR*


1. It takes everyone, not just IT
2. Must have top-down support
3. Plan, Prepare, Test and Revise
4. We must be perfect, all the time. Hackers only need to be right ONCE.

Questions?

Ryan Burns
Cyber Risk Services Manager
Ph: (512) 491-3427
rburns@tmlirp.org