The Myths and Truths about Your Cyber Risk
Your Digital Guides for today...

Ny Brown – Sr. Systems Administrator, TAC
Matt Bruns – Sr. Systems Administrator, TAC
Todd Kisel – Risk Management Consultant, TAC
Robert Ruiz – RMS Associate Director, TAC
Disclaimer

The information presented in this session is for educational purposes only. Coverage and Information Technology (IT) scenarios, checklists, and answers presented are not requirements of coverage, determinations or endorsements of specific software, services or technology companies.

Each potential claim is unique and must be evaluated on its own merit. Coverage as provided by the TAC RMP is subject to the terms and conditions of the specific coverage document.

This session does not satisfy or comply with HB 3834 (86th Legislature) requirement at this time.
Learning Objectives
Myth #1

I am not on social media (Facebook, Twitter, Instagram, etc…) therefore I am not susceptible (or less of a target) to a cyber event.
Myth #2

I have no part in my county’s cyber plan, that is what the IT department is for (and their responsibility).
Truth #1

Risks generally characterized as “cyber” are generally broader than those involving computers or computer networks.

Just because your county government may not maintain or keep electronic records, does not eliminate the risk of a data breach.

A data breach can be digital or physical in nature.
Even though data has not been exposed, it does not mean that a county did not have a cyber security event.
Which Cyber is it?

- **Event** – is any cyber occurrence/happening
- **Incident** – is the act of violating an explicit or implied security policy ([U.S. DHS-CISA](#))
- **Breach** – is the intentional or unintentional release or exposure of sensitive and private data by an unauthorized source, party or individual
IT and Risk Management have to be on the same page!
URGENT: Ransomware Targeting Governmental Entities

August 16, 2019

We have learned of a widespread cyber attack that is targeting governmental entities with ransomware. Please ensure that you are exercising extreme caution in opening emails and attachments, or clicking on links. We also suggest you contact your IT Department and vendor immediately to ensure they are actively monitoring your systems and network for any suspicious activities and that your antivirus and anti-malware programs are actively running.

For more detailed information, visit the Department of Information Resources (DIR) website at www.dir.texas.gov for their notice: "Ransomware Attack Hits Texas Government Entities."

If you have Public Officials Coverage with the TAC Risk Management Pool and are affected, please contact Andrea Beard at 512-745-0253.
Pre-incident Checklist

Home Cybersecurity Checklist

- Install anti-virus protection to safeguard against viruses that can corrupt your system and destroy your data.
- Stay up-to-date on device updates to eliminate bugs and security vulnerabilities.
- Change default credentials to prevent unauthorized and malicious access.
- Use strong passwords that can’t be easily cracked.
- Use a password manager so you can use different passwords without having to remember them all.
- Be cautious of freeware by first ensuring apps are reputable and safe.
- Avoid phishing emails and bad links by deleting suspicious messages from unknown senders.
- Use search engines to find websites to avoid visiting malicious websites due to URL misspellings.

Education Center
Powered by BankersTrust
Education.BankersTrust.com
Member FDIC
At this time, we want to deepen our understanding of Cyber Security with a demonstration of some real world incidents.
USB or Unknown Safety Breach

- Conference giveaways
- Personal storage devices (USB, thumb drive...)
- USB drives a friend shares with you
- USB drive you found on the floor or on a table

What do all these have in COMMON?
## Post-incident Checklist

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact</td>
<td>Contact IT and/or your contracted vendor.</td>
</tr>
<tr>
<td>Notify</td>
<td>Notify and file claim with TAC RMP or your insurance carrier.</td>
</tr>
<tr>
<td>Consult</td>
<td>Consult with Data Breach Coach*</td>
</tr>
<tr>
<td>Implement</td>
<td>Implement your Cyber Resilience/Incident Response plan</td>
</tr>
<tr>
<td>Work</td>
<td>Work with Forensic team and other key stakeholders or vendors</td>
</tr>
<tr>
<td>Begin</td>
<td>Begin mitigation and recovery efforts</td>
</tr>
</tbody>
</table>

*Authorities may need to be notified. Consult your County Attorney and Data Breach Coach*
Cyber Resilience

• Have a plan
• Test the plan
• Identify
• Protect
• Detect
• Respond
• Recover

When you bend with the wind, don’t break in the storm.
Considerations

• Does a Cyber policy cover everything?
  • What if funds are transferred?
  • Who do I call?
• Where do we start?
Privacy or Security Event Liability and Expense Coverage

BASIC COVERAGE DETAILS

• Immediate hands on breach response
• Forensic Investigation
• Public Relations
• Notification and Credit Monitoring (if needed)
• Legal Fees
• Regulatory Proceedings and Penalties
• $2,000,000 limit (as of 10/01/19) subject to deductible

*Contained within the TAC RMP Public Official’s Liability Coverage*
Crime Coverage

BASIC COVERAGE DETAILS

• Employee Dishonesty
• Forgery or Alteration
• Theft, Disappearance and Destruction Robbery and Safe Burglary
• **Computer Fraud and Funds Transfer Fraud**
• Money Orders and Counterfeit Paper Currency
• $250,000 limit subject to $1,000 deductible (no additional cost)
• Higher Crime coverage limits available – ask your RMC

*Contained in TAC RMP Property Coverage Document*
Resources

• eRisk Hub
• TAC RMP Cyber Coverage for Members with Public Officials’ Liability coverage
• TAC Cybersecurity Training for Counties*
• Department of Homeland Security (DHS) Cyber Resilience Review (DHS-CISA)
• Texas Department of Information Resources (DIR)
• TAC Risk Management Consultants

*Pending official requirements from Texas DIR as mandated by HB3834*
# Practical Tips

<table>
<thead>
<tr>
<th>Personal</th>
<th>County</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Password management</td>
<td>• Password management</td>
</tr>
<tr>
<td>• VPN</td>
<td>• VPN, firewall, email filters, etc.</td>
</tr>
<tr>
<td>• Firewall</td>
<td>• Penetration testing (soft)</td>
</tr>
<tr>
<td>• Antivirus</td>
<td>• Software patching</td>
</tr>
<tr>
<td>• Situational awareness</td>
<td>• Cyber incident response plan</td>
</tr>
<tr>
<td>• Anti-malware</td>
<td>• Employee training (ongoing)</td>
</tr>
<tr>
<td>• Common sense approach</td>
<td>• Backups – multiple locations</td>
</tr>
<tr>
<td></td>
<td>• Top-down support</td>
</tr>
<tr>
<td></td>
<td>• County-wide communication &amp; participation</td>
</tr>
<tr>
<td></td>
<td>• Vendor &amp; contract management – cyber liability</td>
</tr>
</tbody>
</table>

*Lists are not meant to be exhaustive and all encompassing*
Cybersecurity Threats: Eight Critical Principles

- Denial-of-service attacks continue worldwide
- Malware still poses a significant threat
- The greatest threat may come from within
- Size doesn't matter
- We're slow to detect and respond to threats
- Ransomware poses a grave risk to availability
- Beware of the social engineer
- The biggest threats aren't found in the headlines

Source: IDC, 2018
Estimated Ransomware Costs – Texas 2019

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

As of August 20, 2019
What is Next...