



# Housekeeping

The presentation will begin at 11 am CST

- Please **mute your computer or phone**
- Please **turn off your cameras** to save bandwidth
- Questions will be answered at the end of the presentation
- *Use the chat box for questions*
- Please complete the surveys that will be emailed after the presentation

# UTSA SBDC

## Center for Government Contracting



South-West Texas Border  
Small Business  
Development Center Network

UTSA SBDC Center for Government Contracting

## *Cyber Threats in 2021*

<http://cgctxsbdc.org/>

(210) 458-2458

---

Institute for  **Economic** Development  
The University of Texas at San Antonio



**UTSA**<sup>®</sup>



South-West Texas Border  
**Small Business  
Development Center Network**

*UTSA SBDC Center for Government Contracting*

# Your Host

**Troy Richardson**  
**Business Development Specialist**  
**UTSA SBDC CGC**  
[Troy.Richardson@utsa.edu](mailto:Troy.Richardson@utsa.edu)



- Air Force Veteran
- DoD Civilian Retiree
- Former Small Business Owner
- Cybersecurity



South-West Texas Border  
**Small Business  
Development Center Network**

*UTSA SBDC Center for Government Contracting*

# UTSA IED



- The UTSA Institute for Economic Development (IED) provides ongoing:
  - Consulting
  - Training
  - Technical research and information services in tandem with University-based assets and resources, and other state, federal and local agencies, to facilitate economic, community, and business development throughout the 79 Counties of South Texas and the Border Region plus Oklahoma and Louisiana.
- [www.iedtexas.org](http://www.iedtexas.org)

Institute for **Economic** Development  
The University of Texas at San Antonio



**UTSA**®



South-West Texas Border

## Small Business Development Center Network

*UTSA SBDC Center for Government Contracting*

# Our Service Areas

Supports a 79-county SBDC Network covering the following areas:

- San Antonio
- Alpine
- Austin
- Corpus Christi
- Eagle Pass
- El Paso
- Laredo
- Rio Grande Valley
- San Angelo
- Victoria



South-West Texas Border  
**Small Business  
Development Center Network**

*UTSA SBDC Center for Government Contracting*

# Our Services

## Services provided...



One on One  
Counseling



Trainings, Town Halls &  
Networking Events

---

Institute for **Economic** Development  
The University of Texas at San Antonio



**UTSA**<sup>®</sup>





South-West Texas Border  
**Small Business  
Development Center Network**

*UTSA SBDC Center for Government Contracting*

# CGC Staff

**Terri Williams, Associate Regional Director**

## TEXAS CYBERSECURITY COMPLIANCE PROGRAM

Victor Malloy, Project Manager

## EMPLOYER SERVICES

Deirdre Pattillo, Project Manager

## CYBERSECURITY FOR SMALL BUSINESS

Troy Richardson, Business Development Specialist

## SBDC COVID BUSINESS RECOVERY ACCELERATOR

Jaime Martinez, Sr. Project Manager

Susannah Munro, Sr. Business Development Specialist

Nestor Astorga, Sr. Business Development Specialist

## SUPPORT STAFF

Clara Chavez, Training Coordinator

Maria Holloway, Web Specialist

Eileen Teves, Marketing Coordinator

Nathan Aguilar, Graphic Designer

Rose Marie Reyes, Administrative Associate

Norma Gomez, Administrative Associate



# CGC Programs



## 1. COVID Business Recovery Accelerator

- Assisting small businesses in the area of COVID business recovery

## 2. Texas Cybersecurity Compliance Program

- A collaboration with the IED, UTSA Center for Infrastructure Assurance and Security (CIAS) and SBDCs throughout the state of Texas to provide the Texas Cybersecurity Compliance Program (TCCP)

## 3. Cybersecurity for Small Businesses

- Provides awareness through training, one-on-one assistance with the cybersecurity action plan development and implementation working with other UTSA specialty centers on cybersecurity

## 4. Small Business Emergency Preparedness

- Assist small businesses with preparing for disasters, business interruptions and being ready for anything

## 5. Employer Services

- Provides direct assistance to small business employers in the areas of employment practices, regulatory compliance, job site safety, drug-free workplace, and effective HR management



# Small Business Essentials

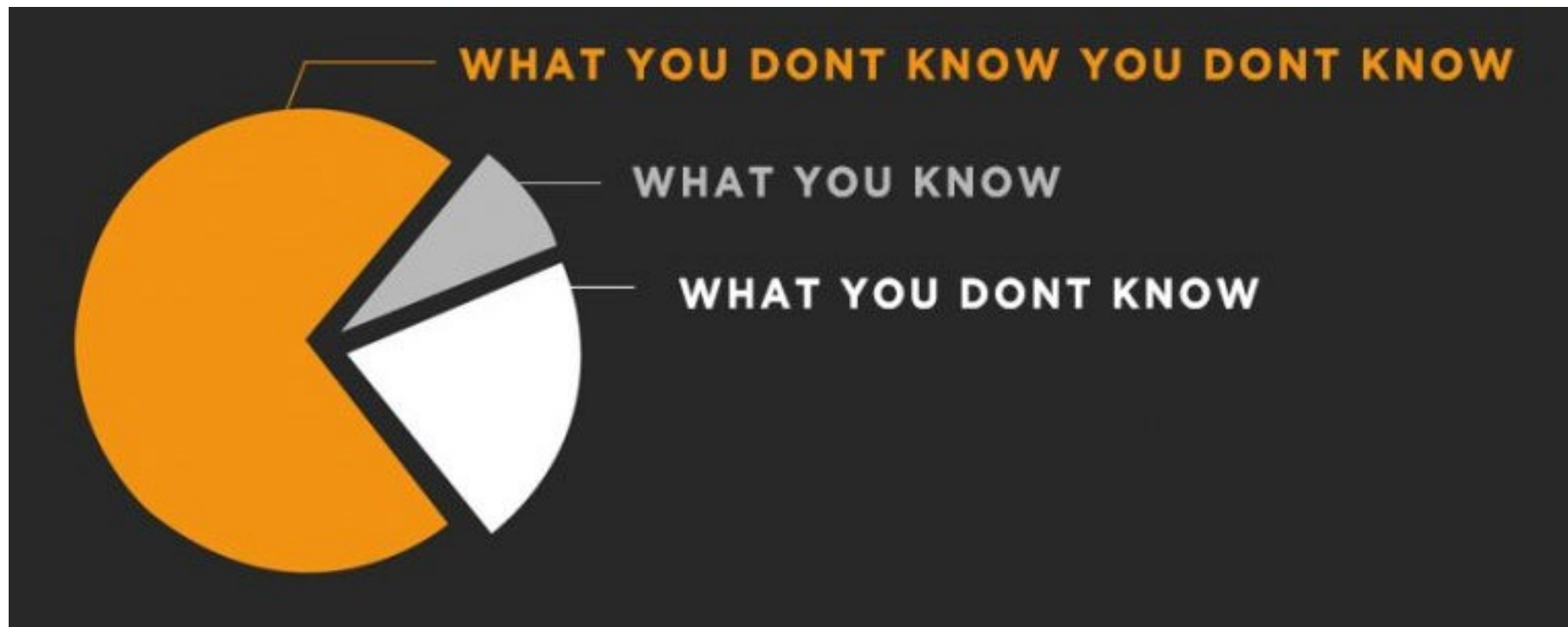
1. Strong business plan
2. Marketing plan / strategy
3. Customer focus and engagement
4. Capital
5. Patience
6. Persistence
7. Cybersecurity

# Agenda

- ✓ Why
- ✓ Common Threats
- ✓ “Emerging” Threats
- ✓ Q & A



# Why?



# COMMON CYBER THREATS

Cyber threats are in the headlines and possibly in your network. Here are some common forms of cyber threats to protect against.

## RANSOMWARE

malevolent software which locks user access by encrypting data using cryptovirology while extorting payment from the victim in order to de-encrypt and restore the files



## MALWARE

malicious software installed on a machine unknowingly and performs criminal actions for a third party



## SPOOFING

email messages sent from a fraudulent account masquerading as a legitimate and trusted source as an attempt to gain access to a user's system or confidential information

# Account Takeover

- A means to information (PII)
  - Accounts can be:
    - Used by the criminal
    - Sold on the dark web
- 
- ✓ Practice good cyber hygiene
  - ✓ Implement MFA
  - ✓ Strong email security solution





# Angler Phishing



- A means to gain access or deploy malware
- Preying on emotions, especially frustration
- ✓ Post your social media practices
  - ✓ How and when you'll respond
  - ✓ What info may be asked of customers
- ✓ Monitor your social media presence





# Business Email Compromise



Employee email account  
is compromised by the  
cybercriminal



Compromised account used  
to notify the supplier's  
customers of a change to  
the invoice payment details



Customer transfers their  
payment to the  
cybercriminal's account



Cybercriminal  
receives the money



# Bill Fraud



- Money is the goal
- Service fee based society and automatic payments
- ✓ Pay based on invoice, not statements
- ✓ Separation of billing duties
- ✓ Manual payments
- ✓ Establish a culture of “trust but verify” in your employees



# Business Invoice Fraud

- Similar to Bill Fraud but target against businesses
  - Money is still the goal
  - Preying on lack of oversight / attention
- 
- ✓ Internal controls i.e. dual approval
  - ✓ Use 3-way matching: PO → Invoice → Receipt
  - ✓ Rotate accounting duties





# Credential Attacks



Credential Dumping  
Credential Reuse Attack  
Credential Stuffing  
Masquerade Attack

- ✓ Implement MFA!
- ✓ Change passwords often



# Cryptojacking

- After computing power / resources
- “Bank tellers” of crypto transactions
- ✓ Practice good cyber hygiene
- ✓ Ad-blocking or anti-cryptomining browser extensions
- ✓ Endpoint protection (AV / AM)



# Drive-by Download



- Exposure to multiple threats
- No clicking by users required
- ✓ Updates and system patches
- ✓ Use a browser extension that warns against potential harm
- ✓ Updates / patch regularly
- ✓ Disable java and java script



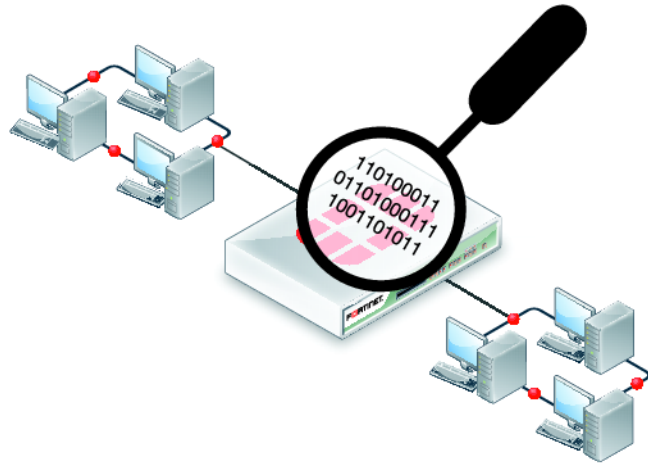
# IoT Threats

- Device access, then increased access
- Easy entry point, often “forgotten”
- ✓ Change default passwords!!!!!!!
- ✓ Disable Universal Plug and Play (UPnP)
- ✓ Separate network for IoT devices
- ✓ Update firmware





# Network Sniffing



- Seeking information and clues
  - Digital equivalent of wiretaps
  - Not new, but more lucrative due to the amount of information on networks now
- 
- ✓ Encrypt traffic (VPNs)
  - ✓ Avoid HTTP websites (use HTTPS)
  - ✓ Stay off unsecure WiFi networks

# Shadow IT

- SaaS most common vulnerability
  - Cloud storage, Google Apps, Concur
  - Used for convenience and productivity
- 
- ✓ Baseline configurations
  - ✓ Access controls
  - ✓ Training and awareness
  - ✓ Auditing and monitoring





# System Misconfiguration



- Incorrectly configured, or missing, security controls
  - Vulnerable software / hardware
  - Use of default accounts
- 
- ✓ Baseline configurations
  - ✓ Update / patch regularly
  - ✓ Monitor logs

# Typosquatting

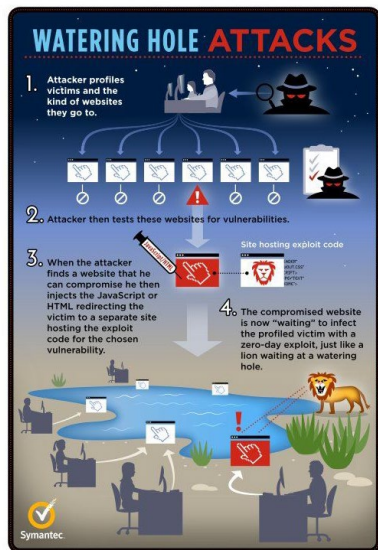
- Purposely misspelled domain names
  - Deliver malware or to make money
- 
- ✓ Protect your domain
    - ✓ Cipher Box domain protection for example
  - ✓ Purchase all related domain URLs
  - ✓ Run your own DNS Server

## Examples of Typosquatting

Real Domain Targeted	Typosquat Domain Example
www.github.com	www.gIthub.com
www.google.com	www.g <u>o</u> gle.com
www.amazon.com	www.am <u>o</u> zon.com
www.victoriasecret.com	www.victoriasecret.com
www.homedepot.com	www.homed <u>e</u> pot.com



# Watering Hole



- Social Engineering-esque
  - Relies on predictability
- 
- ✓ Anti-Malware on endpoints
  - ✓ Utilize enterprise web gateways
  - ✓ Strong email security solution
  - ✓ Utilize virtual based or a secure cloud browser





South-West Texas Border  
**Small Business  
Development Center Network**

*UTSA SBDC Center for Government Contracting*



---

Institute for  **Economic** Development  
The University of Texas at San Antonio



**UTSA**<sup>®</sup>



# Building the Texas Economy One Business At a Time

UTSA SBDC

Center for Government Contracting

<https://cgc.txsbdc.org>

(210) 458-2458



Each program within the Institute is funded through various state and federal programs,  
and respective service areas differ according to that particular program's mission.