ENTREPRENEURSHIP
ADVANTAGE

BUILDING DIGITAL RESILIENCY

October 29, 2020

Welcome

Heidi Pickman

CAMEO

VP, Programs and Policy

General Info

- Everyone's audio is muted
  - Zoom menu --- drag cursor down screen.
  - Mic icon on left.
  - Chat box.
- We are recording and you are free to share. We will send all registrants a link as soon as we can
- You will receive a copy of today's slides.

CAMEO Updates

- CA Rebuilding Fund: Train the Trainer (Nov 12)
- Managing Lending Risk in Times of Crisis (Nov 19)
- Microlending Essentials
- NorCal Regional Meeting (Dec 3)
- Sacramento Regional Meeting (Dec 8)
- Coronavirus Resources for Small-Business

Frank Stokes

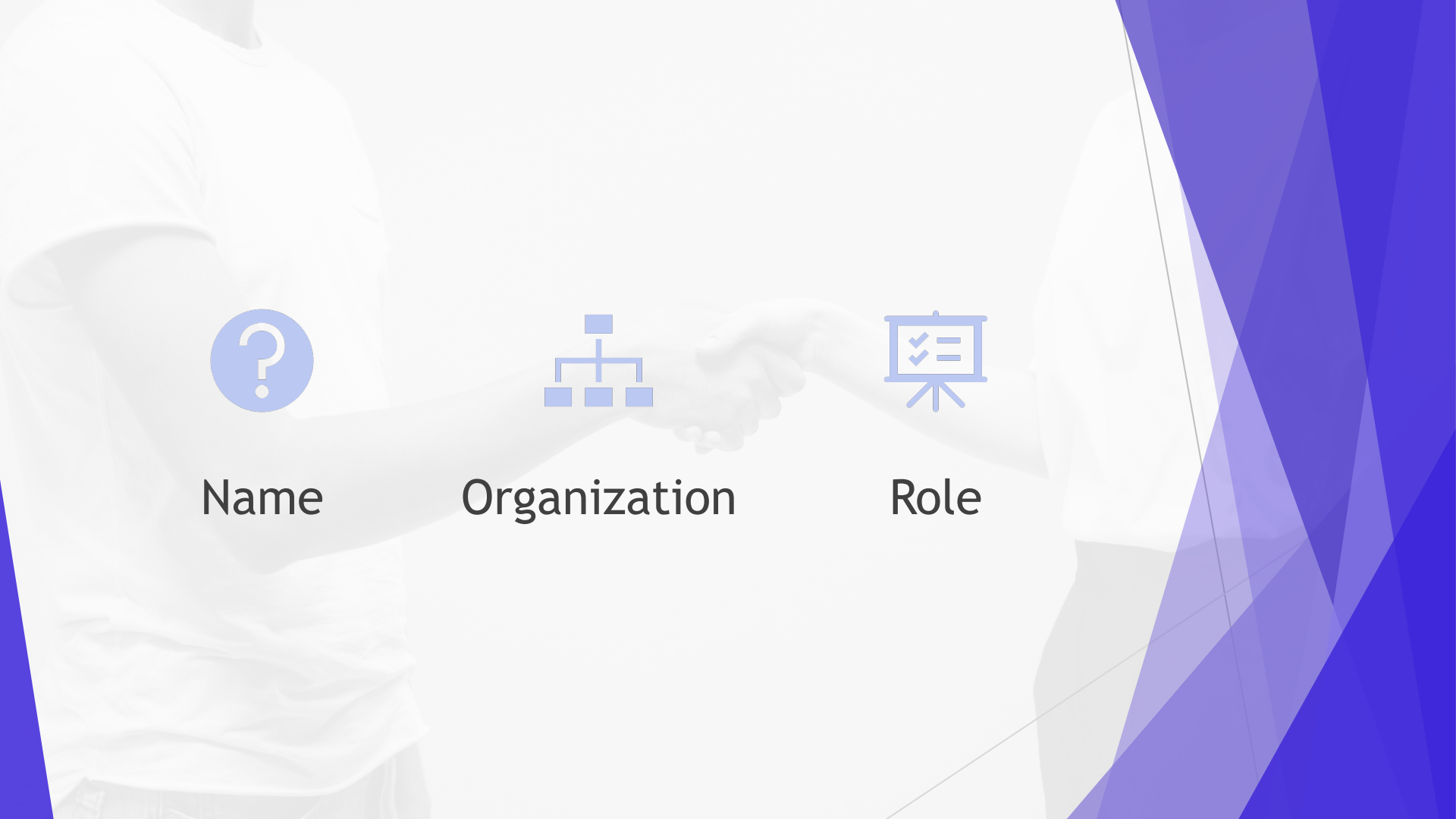
BEST Mobile Accelerator

EA Steering Committee

ENTREPRENEURSHIP ADVANTAGE

Agenda

- Building Digital Resiliency
- Q&A and discussion



Name

Organization

Role

Purpose

Entrepreneurship Advantage

- Create economic opportunity for entrepreneurs and small businesses in LA County by connecting human, technical and capital resources through regional collaboration.

Virtual Meetups

- Bring EA members to discuss best practices, strategies, and challenges in light of COVID-19's effects on the small-business sector

Digital Resiliency and COVID-19

- Responses to COVID-19 have speeded digital adoption by several years – and many executives believe that these changes could be long-term (McKinsey & Company)
- According to a recent SBA survey, nearly 9 in 10 business-owners felt their business was vulnerable to cyber-attack. However, many small businesses can't afford professional IT solutions, don't have time to focus on cybersecurity, or simply don't where to start.
- Today, we'll focus on how you can improve digital resiliency in your organization or business

JESSE TORRES
PRINCIPAL
ARROYOWEST LLC
& CAMEO BOARD CHAIR
Jesse.Torres@arroyowest.com

The Essentials of Digital Resiliency

ABOUT JESSE

linkedin.com/in/jessetorresca

Jesse Torres is Principal for ArroyoWest LLC, a minority-owned consulting firm based in Los Angeles County. Primary practice areas include economic and workforce development, procurement and supplier diversity, disaster preparedness and general business strategy.

Torres is the former principal Small Business Advocate for the State of California and Deputy Director of Small Business and Innovation for Governor Brown's Office of Business and Economic Development (GO-Biz). During his three-year tenure at GO-Biz, Torres was successful in securing more than $108 million in state general funds to provide match and capacity building grants for the federal small business TA providers in California. Torres also administered a portfolio of high-profile programs including the state's Innovation Hub (iHub) Network, the state's defense supplier diversification and cyber resiliency program, CASCADE, the California Cybersecurity IT Health Advisory Board, and the California Cyber Innovation Challenge. Torres also led small business recovery efforts for GO-Biz following major disasters including the destructive 2017 Northern California Tubbs and Southern California Thomas Fires and Montecito mudslides.

Torres is Chair of the Board for California Association for Micro Enterprise Opportunity, Advocacy Chair for Union Station Homeless Services, and was appointed by Los Angeles Mayor Eric Garcetti to the City's seven-member Small Business Commission. Torres also serves as a member of the board for Associated Students UCLA, Northern California SBDC Network, Scale LA, SEE-LA and is a member of the Los Angeles Cyber Fraud Task Force administered by the U.S. Secret Service.

Ponemon Institute: 2018 State of Cybersecurity in Small and Medium Size Businesses – 1,045 SMEs surveyed.

- 67% of respondents suffered a cyberattack
- Majority said the data breach was due to a negligent employee or independent contractor.
- Mobile devices were the most vulnerable entry points to companies' computer networks.

Digital Resiliency as Part of Preparedness Planning

OUTSMART DISASTER

https://outsmartdisaster.com/

Objectives:

- Improve communication of disaster hazard science and engineering for use in decision making processes
- Inform actions to reduce disaster risks
- Build business capacity to respond to and recover from disasters

Prepare & Anticipate	Support Key Stakeholders	Secure & Protect	Adapt & Recover	Rinse & Repeat
Document your business functions Identify impacts of disruption	Recognize key relationships with suppliers, vendors, partners Train and care for employees	Strengthen your facilities Safeguard data and vital documents	Understand your insurance and finances Document your contingency options	Establish a process to continually re-assess risks at regular, pre-determined intervals and trigger points

RISK ASSESSMENT

1. Identify and Describe Hazards (Natural or Manmade)

2. Identify Assets (Who or What will be affected?)

3. Analyze Risks
   a. Historical Occurrences
   b. Exposure Analysis
   c. Scenario Analyses

4. Summarize Vulnerability

5. Incorporate Changes

SCENARIO ANALYSIS

	SCENARIO A 3 mos. business interruption, 15% revenue loss	SCENARIO B 6 mos. business interruption 25% revenue loss	SCENARIO C 12 mos. Business interruption 40% revenue loss
PLAN A			
PLAN B			
PLAN C			

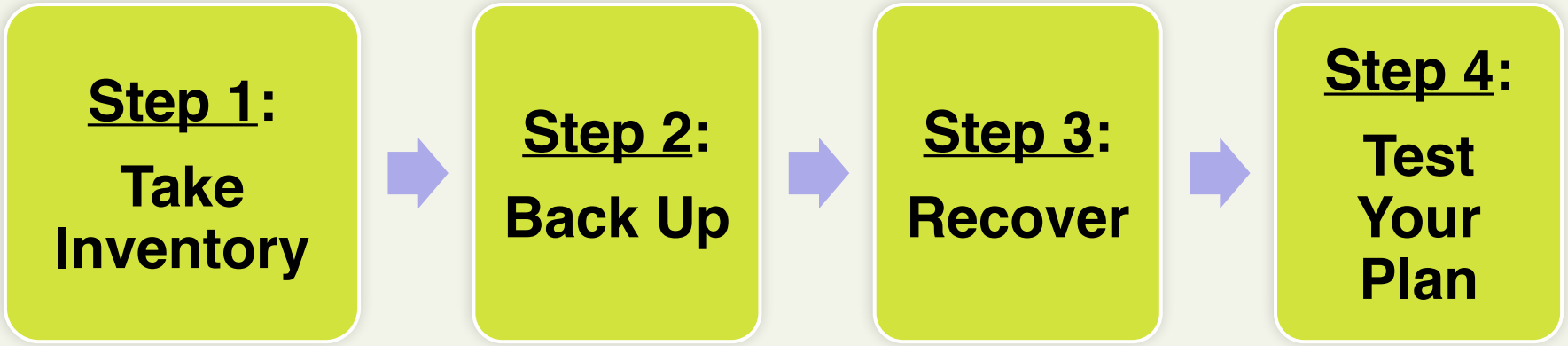
The Resilient Business Challenge

https://outsmartdisaster.com/for-businesses/resilient-business-challenge/

Safeguard your data and vital documents

OUTSMART DISASTER

Safeguard your data and vital documents



OUTSMART DISASTER

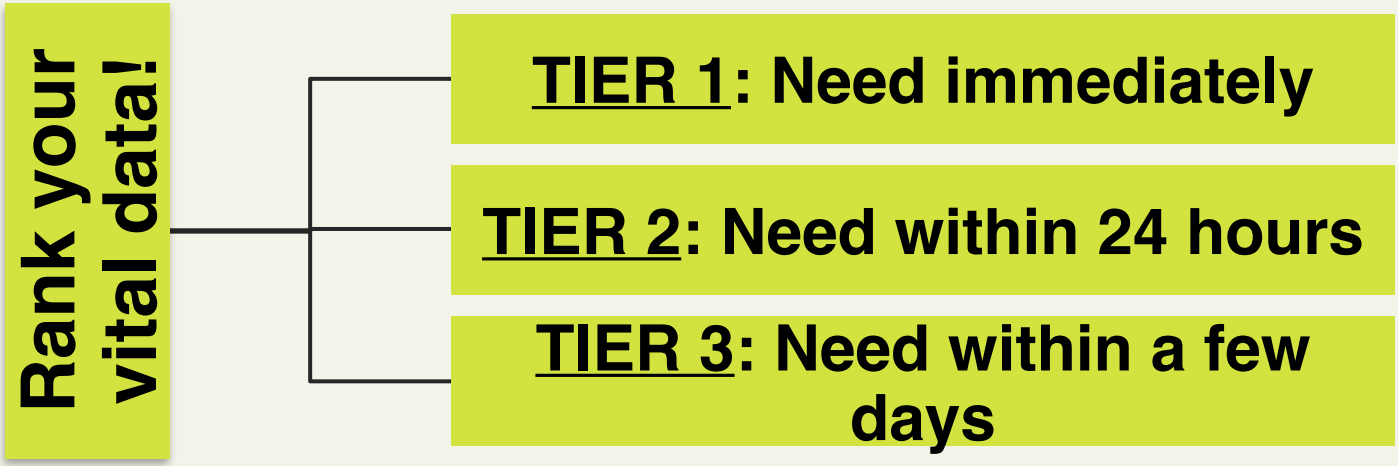
Step 1: Take Inventory

What are vital records?

- Critical to resuming business operations
- Certain legal and financial documents
- Protects your key stakeholders
- Difficult or expensive to reproduce

OUTSMART DISASTER

- Where is your vital data stored?



Vital Records Classification Checklist

OUTSMART DISASTER

Step 2: Data Backup

- Backup at secure location
- Ensure security of backup data
- Regular or automatic backups
- Keep all sources updated
- Include business resiliency plan

OUTSMART DISASTER

Step 3: Data Recovery

Your plan should consider:

- Speed: How fast you'll need access
- Cost: Affordability of your preferred strategy
- Privacy/Security: How sensitive is your data?
- Manpower: Who will implement and how

OUTSMART DISASTER

Step 4: Test Your Plan

Set a testing schedule

Gauge time needed

Access from different locations

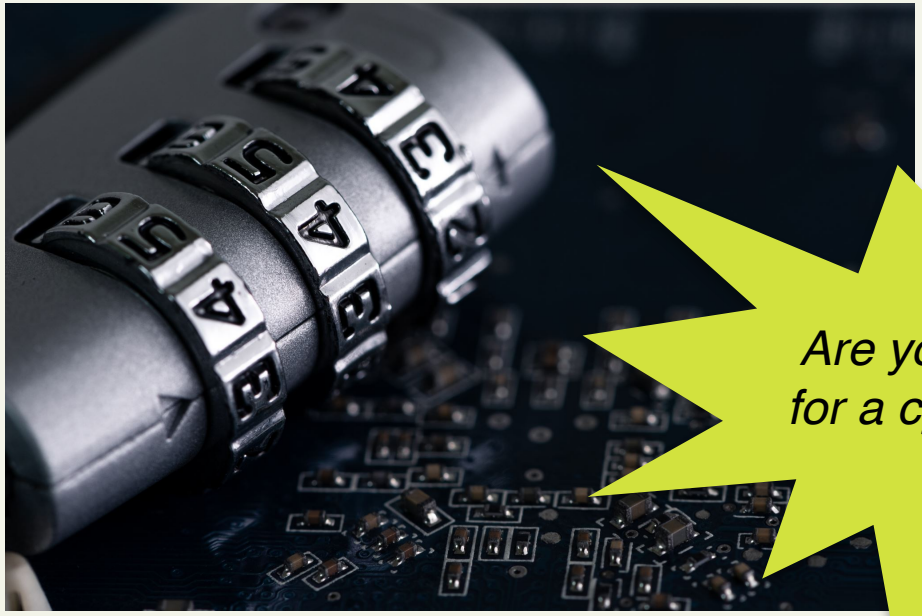
Test Runs!

Consider different scenarios

Correct for weaknesses

OUTSMART DISASTER

Safeguard your data and vital documents



Are you prepared for a cyber attack?

OUTSMART DISASTER

Cyber Security Considerations

Does your business dedicate employees to:

- Manage your network?
- Engage with third party vendors for hardware, software, cloud solutions?

Develop a strategy for:

- Physical security
- Boundary Protection
- Encryption

OUTSMART DISASTER

Cyber Security Considerations

Network Segmentation

- If a device or machine is comprised, make sure to prevent other parts of your network from being impacted.

Workload Protection

- Use anti-virus and vulnerability management tools that regularly scan web sites for vulnerabilities.

Asset and Software Inventory

- Know all your products and devices and keep them patched and secured.

Data Protection Impact Assessment (DPIA)

- A tool or process that allows for identification and classification of risks within a business
- Helps determine if processes would compromise the privacy of your customers, staff, or anyone on whom they hold, collect or process data.

OUTSMART DISASTER

9 Key Considerations for a DPIA

1. Does the business need to carry out a DPIA for this project/ process?
2. Describe how the data will be gathered/processed.
3. Consider if external advice is needed.
4. Assess the necessity and proportionality of gathering/ processing the data.

OUTSMART DISASTER

9 Key Considerations for a DPIA (continued)

5. Identify and assess risk of gathering/processing the data, especially if those risks affect individuals.

6. Identify any required measures to mitigate the identified risk.

7. Sign off and record the outcomes of any decisions made.

8. Integrate these outcomes into the overall business plan/objectives.

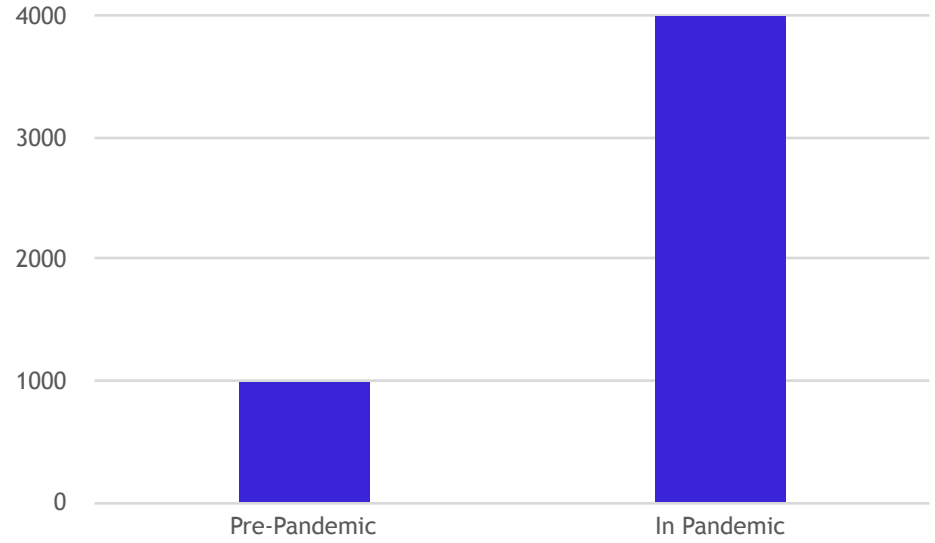
9. Keep these outcomes under review.

OUTSMART DISASTER

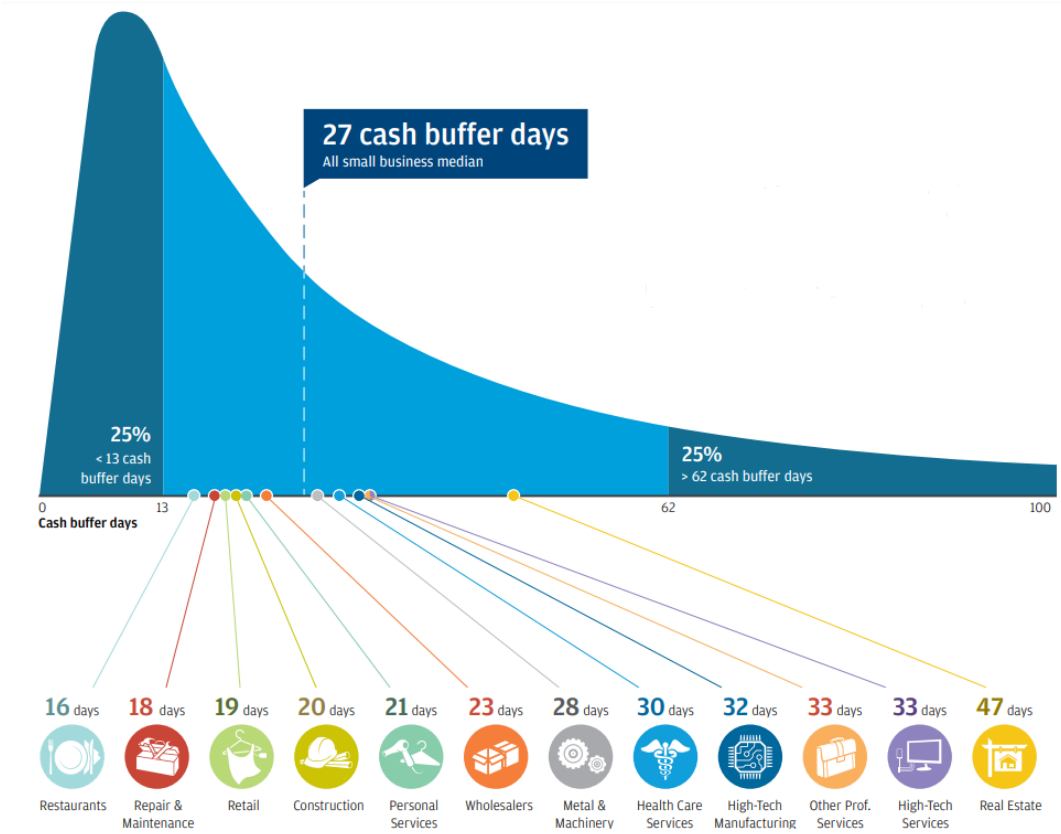
So What

Cyberattack on the rise!

Cybersecurity Complaints to FBI Internet Crime Complaint Center (IC3)



The median small business holds 27 cash buffer days in reserve.



JP Morgan Chase & Co. Institute

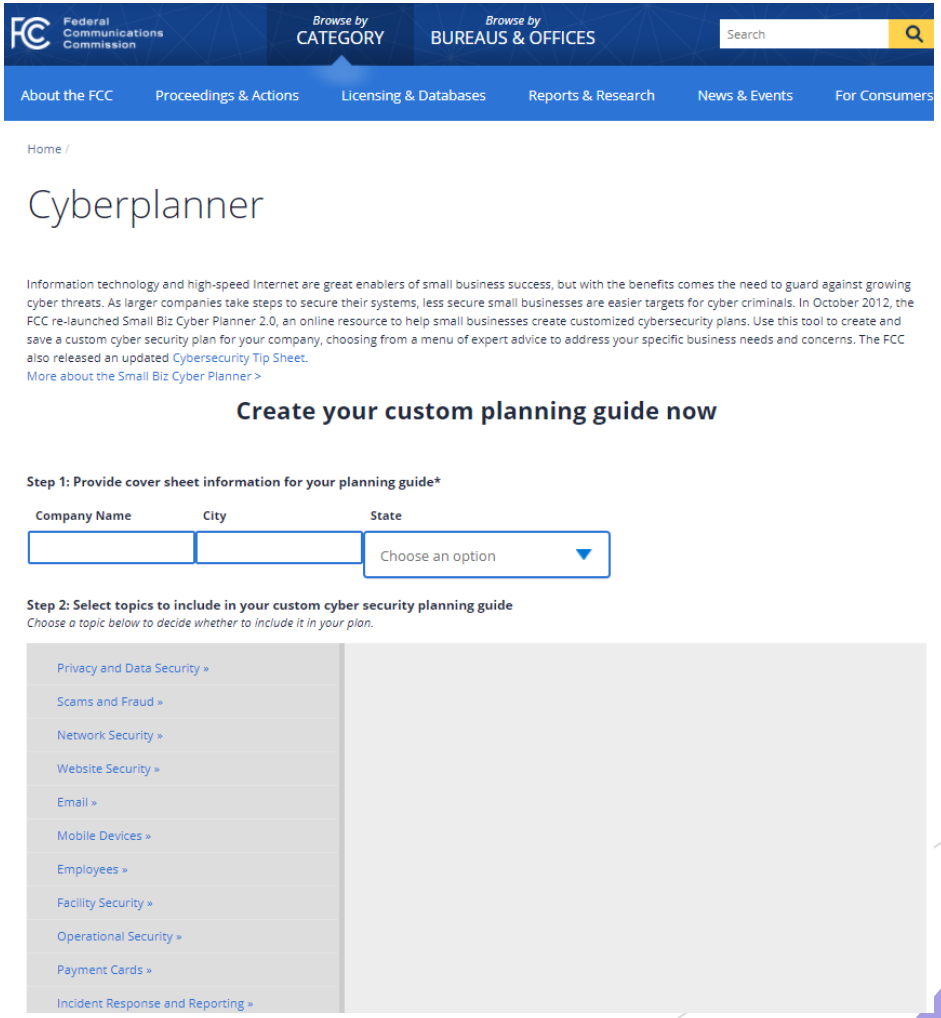
Keep Learning, Exploring and Practicing

U.S. Small Business Administration - Stay safe from cybersecurity threats
https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats#section-h

Cybersecurity best practices

- **Train your employees**
  - Employees and emails are a leading cause of data breaches for small businesses because they are a direct path into your systems. Training topics to cover include: Spotting a phishing email, using good browsing practices, avoiding suspicious downloads, creating strong passwords, protecting sensitive customer and vendor information

- **Maintain good cyber hygiene**
  - **Use antivirus software and keep it updated**
  - **Secure your networks**
    - Using a firewall and encrypt information. If you have a Wi-Fi network, make sure it is secure and hidden.
  - **Use strong passwords**
    - Includes: 10 characters or more; at least one uppercase letter; at least one lowercase letter; at least one number; and at least one special character
  - **Multifactor authentication**
  - **Protect sensitive data and back up the rest**
    - Regularly back up the data on all computers. Critical data includes word processing documents, electronic spreadsheets, databases, financial files, human resources files, and accounts receivable/payable files. Back up data automatically if possible, or at least weekly, and store the copies either offsite or on the cloud.
    - **Secure payment processing**
      Work with your banks or card processors to ensure the most trusted and validated tools and anti-fraud services are being used.
    - **Control physical access**
      Prevent access or use of business computers by unauthorized individuals.

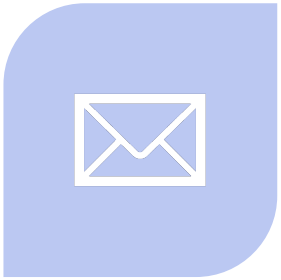


https://www.fcc.gov/cyberplanner

Get Involved

CONNECT WITH US ON LINKEDIN

JOIN OUR COLLAB BY FILLING OUT AN INTEREST FORM



SEND INFO ABOUT YOUR ORG AND UPCOMING EVENTS TO MCRUZ@CAMEONETWORK.ORG