Cyber Storm Warnings

A Cybersecurity Simulation for County Government Leaders

THE COUNTY OF BEACHSIDE FLORIDA

CYBER FLORIDA at the UNIVERSITY OF SOUTH FLORIDA

FAC All About Florida FLORIDA ASSOCIATION OF COUNTIES

Simulation Learning Objectives

- **Get to know enough to be dangerous!**
  - **Realize that cyber has mission implications**
  - **And that challenges are not just technical ones**
- **Know that ultimately you are accountable!**
  - **Identify cost-effective things you can do**
  - **As well as where you need cyber expertise**
  - **And where/how to get it**

Basic Netiquette

- **During Plenary Sessions:**

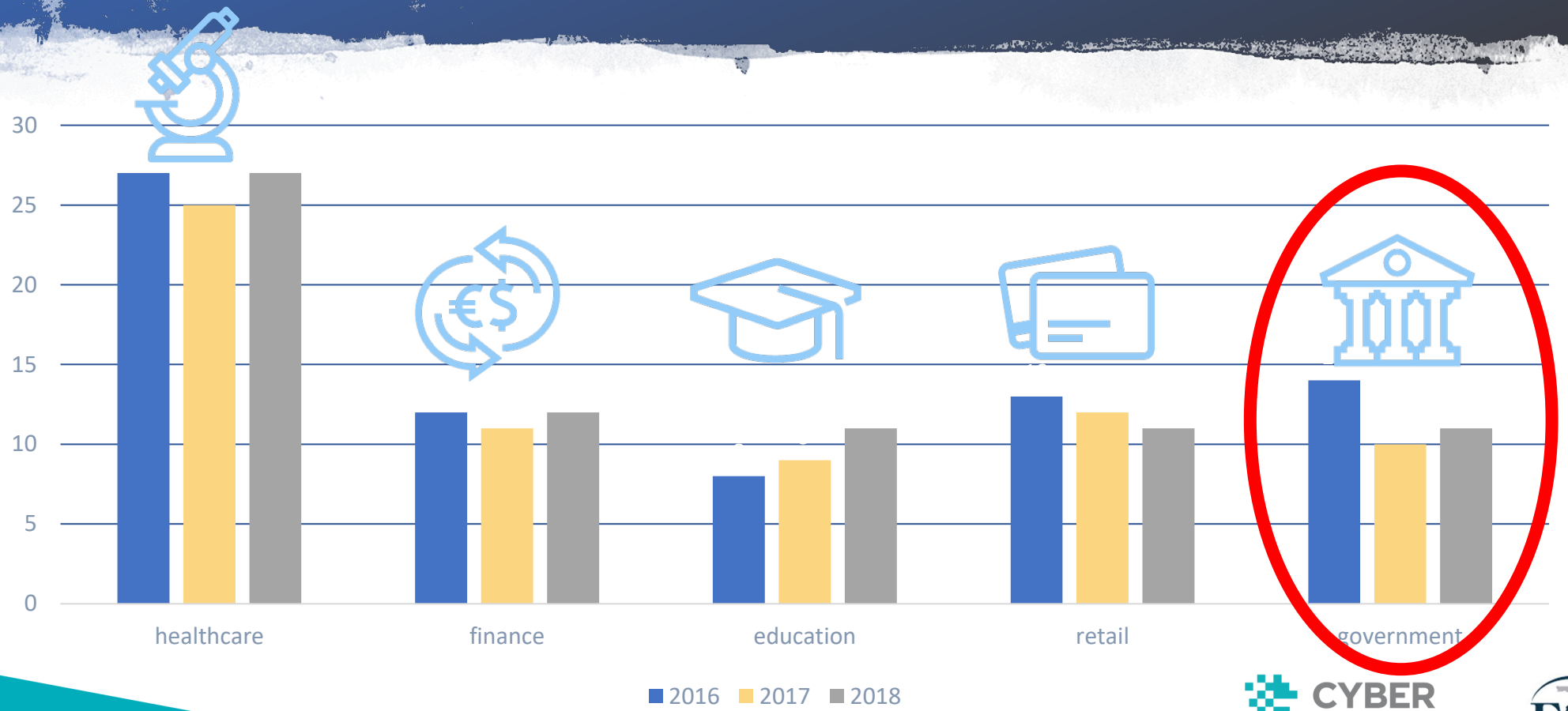
  Keep your **mic muted** unless recognized to speak; keep your **video link open**

- **To Be Recognized to Speak**

  In the “Participants” box, click the Raise Hand icon to the right of your name

- **To Ask Questions, Use Your ‘Chat’ button**

Why Worry About Cybersecurity?



Why Worry About Cybersecurity?

Financial Systems:	**JP Morgan (RUS)**
Fraud/ID Theft	**IRS (UNK)**
Education:	**Dade-County Schools**
Industrial Controls:	**Estonia, ARAMCO, Iran[2]**
All of the above:	**Sony (PRK)**
Local Government:	**Atlanta, Baltimore**

Why Worry About Cybersecurity?

Supply Chain:	**Home Depot (CCs)**
Insider Threat/HR:	**OPM (PRC), NSA (Snowden)**
Intellectual Property:	**Lockheed (PRC), NYC Lawyers**
Physical Security:	**Buckshot Yankee (UNK)**
e-Commerce:	**Bank of America DDOS (IRN)**
Public Policy	**Ft. Lauderdale (Anonymous)**

Why Worry About Cybersecurity?

Pensacola

Collier County

Volusia County

Riviera Beach

FL Division of EM

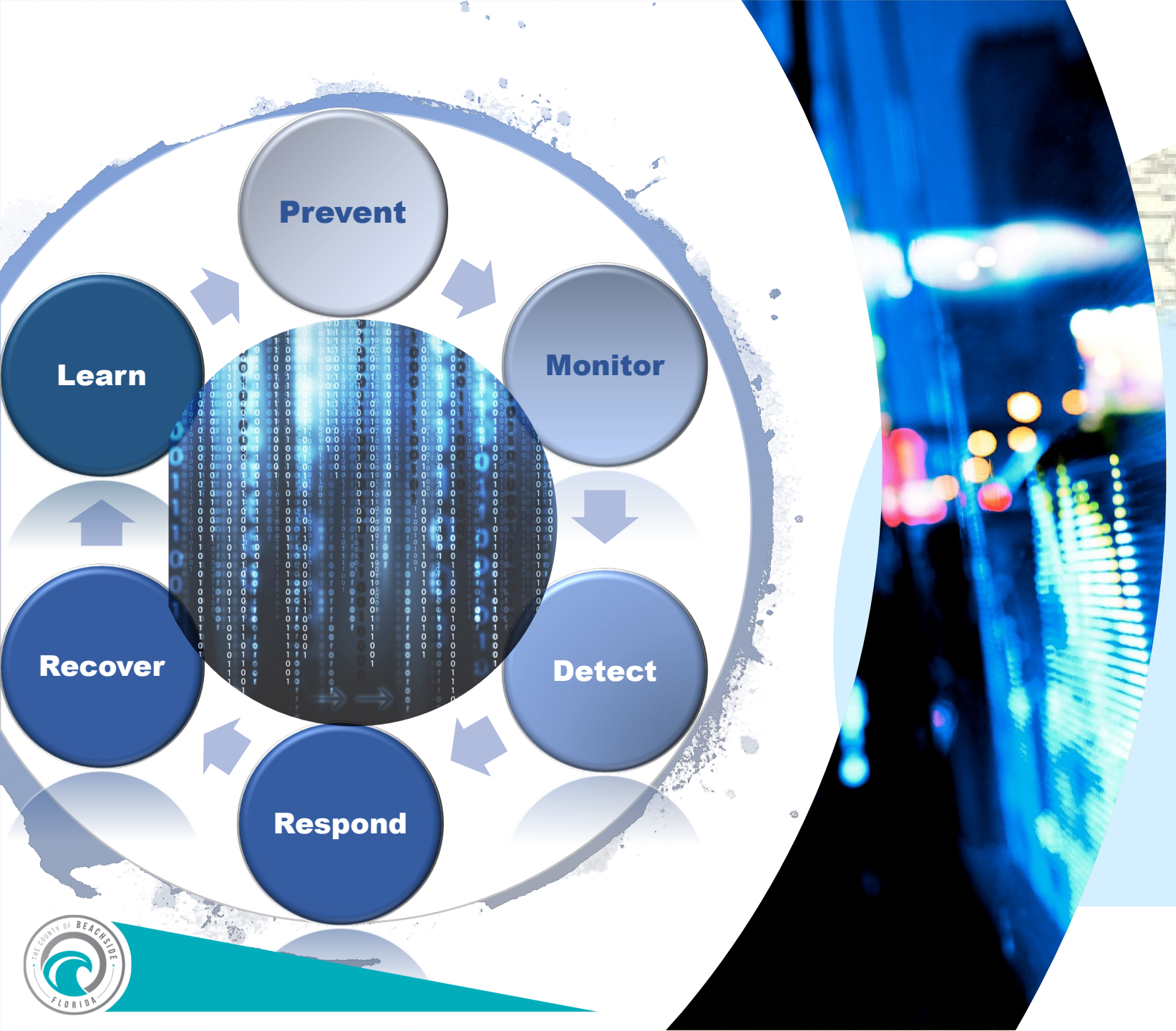
Data Loss

Disruption

Destruction

Disinformation

Deception



Anatomy of a Cyber Attack

- ✓ Prevent
- ✓ Monitor
- ✓ Detect
- ✓ Respond
- ✓ Recover
- ✓ Learn

CYBER FLORIDA at the UNIVERSITY OF SOUTH FLORIDA

FAC All About Florida FLORIDA ASSOCIATION OF COUNTIES

Cyber Storm Warnings:
The Set-Up

Our scenarios are based on the 'real-life' experiences of various public/private sector organizations and takes place in two Acts

- ✓ Act 1: Storm Warnings (a week before the Storm)
- ✓ Act 2:Category 5…the Storm Hits (the first 8 hours)
- ✓ Played out on a compressed time scale

Each team member should be assigned a role that may not necessarily equate to your position or experience

- ✓ But don't let your assigned role inhibit your input
- ✓ Pay attention to your equities and motivations
- ✓ Observe how you set priorities, make decisions

THE COUNTY OF BEACHSIDE FLORIDA

CYBER FLORIDA at the UNIVERSITY OF SOUTH FLORIDA

FAC All About Florida FLORIDA ASSOCIATION OF COUNTIES

Ground Rules and Assumptions

- Don’t fight the scenarios; they’re real, but…
- No ‘book’ answers, just challenges
- Unpredictable things happen…work with them
- Be ready to make decisions with imperfect info
- Don’t worry about struggling…safe to practice, fail
- Play your role…nothing you say/do is ‘personal’
- Nor is anything for attribution!

Welcome to

Beachside, FL

A Growing Gulf Coast County

Population: 70,000

- Fixed income retirees…Snow Birds and Boomers
- Established African-American community
- Growing number of Latino refugees from Maria

Stagnant but diversifying economy

- Near major state university
- Tourism, tech start-ups, ‘work from home’ professionals

County Commission form of government

- Mayor and five-person Council are part-time
- CM terminated for cause several months ago
- HR Director named as Acting while litigation, search proceed

Meet Beachside's Senior Leadership Team...

HR Director/Acting CA

Chief Administrative Officer

Chief Financial Officer

Director of Info Tech

Director of Public Safety

Public Information Officer

County Administrator/
Deputy CA (Vacant)

Director of Economic Development

Director of Public Works

Act 1 – Storm Warnings: 3:30 PM August 20, 2024

Chapter 1: An Anonymous Insider

An EAP Counselor has identified potential ‘insider threat’

- A County IT employee has contacted EAP contractor confidentially
- Has admitted to severe gambling, indebtedness problems
- Has ‘all access’ pass to County’s PII, systems but no evidence of criminal intent
- EAP Counselor refuses to reveal identity

What (if anything) do you do?

Act 1 – Storm Warnings: 3:30 PM August 20, 2021

15 Minutes to Discuss

Potential Insider Threat

Billing Breach

Ransomware, Part 1

Counselor IDs potential insider threat

- A County IT employee contacts EAP contractor
- Confidentially admits to gambling, indebtedness

  Has ‘all access’ pass to County’s PII, systems
- EAP Counselor refuses to reveal identity

What are your options?

Act 1 – Storm Warnings: 2:25 PM August 22, 2024

Chapter 2: Beachside Billing Breach

County's Billing and Payment System is Compromised

- Beachside contracts with EZ Collect, Inc. to bill, collect fees
- EZ runs proprietary software on its servers, with citizen access via portal
- As far as citizens know, this is Beachside's system…and their PII has been stolen
- And one of the victims also happens to be the Commission Chairman's elderly mother!

What (if anything) do you do?

Act 1 – Storm Warnings: 2:25 PM, August 22, 2024

15 Minutes to Discuss

Potential Insider Threat

Billing Breach

Ransomware, Part 1

Billing/Payment System is Compromised

- Beachside contractor EZ Collect bills, collect fees
- EZ runs on its servers, citizens access via portal
- As far as citizens know, their PII has been stolen
- And one of the victims: The Mayor's elderly mother!

What are your options?

Act 1 – Storm Warnings: 8:57 PM, August 23, 2024

Chapter 3: Ransomware, Part 1

County's outsourced water treatment plant hit by 'ransomware'

- Administrative, SCADA systems have been shut down
- Hacker wants 'just' $50,000 in Bitcoin to restart
- No impact on treatment operation
- Contractor wants County financial, other assistance

What (if anything) do you do?

Act 1 – Storm Warnings: 8:57 PM August 23, 2-24

15 Minutes to Discuss

Potential Insider Threat

Billing Breach

Ransomware, Part 1

Water treatment plant hit by ‘ransomware’

- Administrative, SCADA systems have been shut down
- Hacker wants ‘just’ $50,000 to restart
- No impact on treatment operation
- Contractor wants County financial, other assistance

What are your options?

Storm Warnings: August 2024

Intermission

Fast-Forward to August 29, 2024

Act 2 – The Storm Hits: 6:30 PM August 29, 2024

Chapter 4: Dark Web Fire Sale

Citizen PII is up ‘For Sale’ on the Dark Web

- County’s internal systems have been breached by malware
- Hacker has stolen citizen bank accounts, credit cards, SSN’s, passwords, etc.
- Sample posted on Dark Web verifies theft…for sale to the highest bidder
- Breach traced to ‘click’ on seemingly innocuous electronic Public Records request

What (if anything) do you do?

Act 2 – The Storm Hits: 6:30 PM, August 29, 2024

15 Minutes to Discuss

Dark Web Fire Sale

Email Infection

Public Records Penetration

PII 'For Sale' on the Dark Web

- County's internal systems breached by malware
- Bank accounts, credit cards, SSN's, passwords stolen
- Sample verifies theft…for sale to the highest bidder
- Breach traced to 'click' on Public Records request

What are your options?

Act 2 – The Storm Hits: 4:48 PM August 30, 2024

Chapter 5: They're in Our Email!

Employees Report Interrupted/Corrupted Emails

- Using County-issued (and regulated) 'smart phones'
- Plus spear-phishing attacks that appear to come from Help Desk
- External, 'transactional' Web sites are also blocked as a result of DDOS attack
- Irate citizens are threatening consequences 'at the ballot box'

What (if anything) do you do?

Act 2 – The Storm Hits: 4:48 PM August 30, 2024

15 Minutes to Discuss

Dark Web Fire Sale

Email Infection

Ransomware, Part 2

Employees Report Corrupted Emails

- Using County-issued devices
- Plus spear-phishing attacks ‘from’ Help Desk
- External also blocked by DDOS attack
- Irate citizens: Consequences ‘at the ballot box’

What are your options?

Act 2 – The Storm Hits: 9:00 AM September 2, 2024

Chapter 6: Ransomware, Part 2

Hackers Claim to Possess Highly Sensitive/Confidential Info

- Embarrassing ‘personal’ emails from government servers
- Confidential home addresses of County’s law enforcement officers and dependents
- And control of the County’s Emergency Operations Center
- All held for ransom for $1.0M in Bitcoin

What (if anything) do you do?

Act 2 – The Storm Hits: 9:00 AM, September 2, 2024

15 Minutes to Discuss

SCADA Attack

↓

Dark Web Fire Sale

↓

Ransomware, Part 2

Hackers have Confidential Info

- Embarrassing ‘personal’ emails
- Home addresses of County’s LEOs, dependents
- Control of the County’s EOC
- All held for ransom for $1.0M in Bitcoin

What are your options?

Epilogue:
8:38 AM, September 6, 2024

Back to the Future

If We Went Back, What Would We Do?

- Defense ‘Skunk Works’ has proposition
- Send team back in time (pre-attack)
- Have a chance to start over
- And for some, ‘get out of jail’

…What Have We Learned?

Creating a Cyber-Secure Culture…Why?

80%+ cyberattacks are self-inflicted

- Witting: Disgruntled employees, off-duty misconduct
- Unwitting: Data spills, spear-phishing, poor cyber ‘hygiene’

And your ‘Attack Surface’ is vast…

- Citizens, customers, PIGs and Public Record requests
- Employees, contractors, vendors
- Mobile devices, laptops, Web sites, emails/attachments, etc.

It’s all about the ‘Wetware’

Creating a Cyber-Secure Culture…What?

- ✓What's valued, important, second nature
- ✓Who and what gets attention
- ✓Spoken and unspoken understandings
- ✓What we talk about and how
- ✓The rules we observe, and don't
- ✓What gets rewarded, sanctioned

THE COUNTY OF BEACHSIDE FLORIDA

CYBER FLORIDA at the UNIVERSITY OF SOUTH FLORIDA

FAC All About Florida FLORIDA ASSOCIATION OF COUNTIES

Creating a Cyber-Secure Culture…How?

What you and your senior leadership team can do

- ✓Training and education + practice, practice, practice
- ✓Reward policies, practices…and informal recognition
- ✓Peer champions, self-report amnesty, etc.
- ✓Performance measures (what gets measured gets done)
- ✓Staff meetings, communications, consequences
- ✓Gamification, ‘reverse’ social engineering