CYBER SECURITY IN LOCAL GOVERNMENT.

RAY DESJARDINS, CGCIO

IT SENIOR DIVISION MGR, CHARLOTTE COUNTY

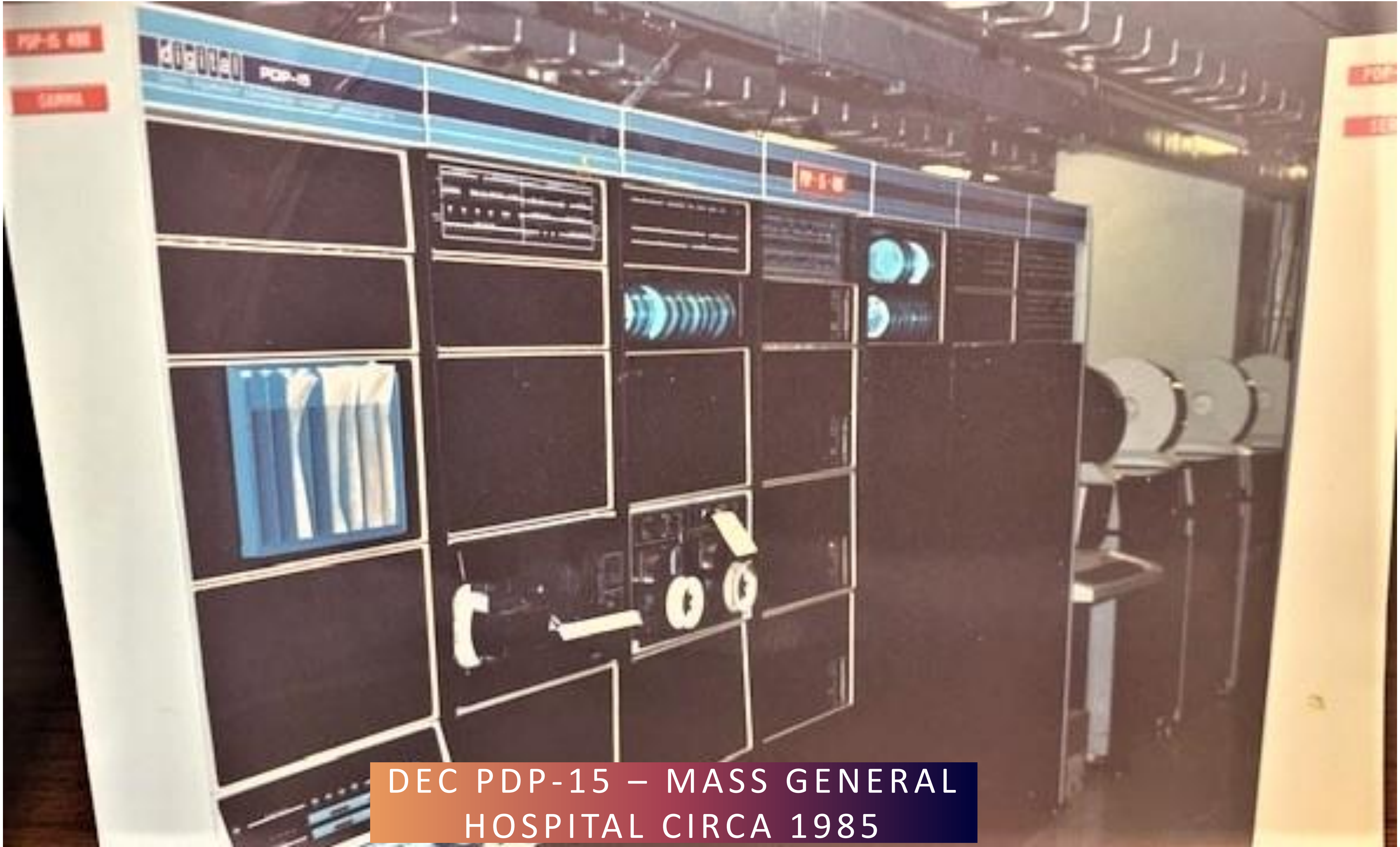
AGENDA

- ➢ INTRODUCTION
- ➢ CURRENT STATE
- ➢ WHAT DOES IT MEAN FOR LOCAL GOVERNMENT
- ➢ WHAT CAN/MUST WE DO

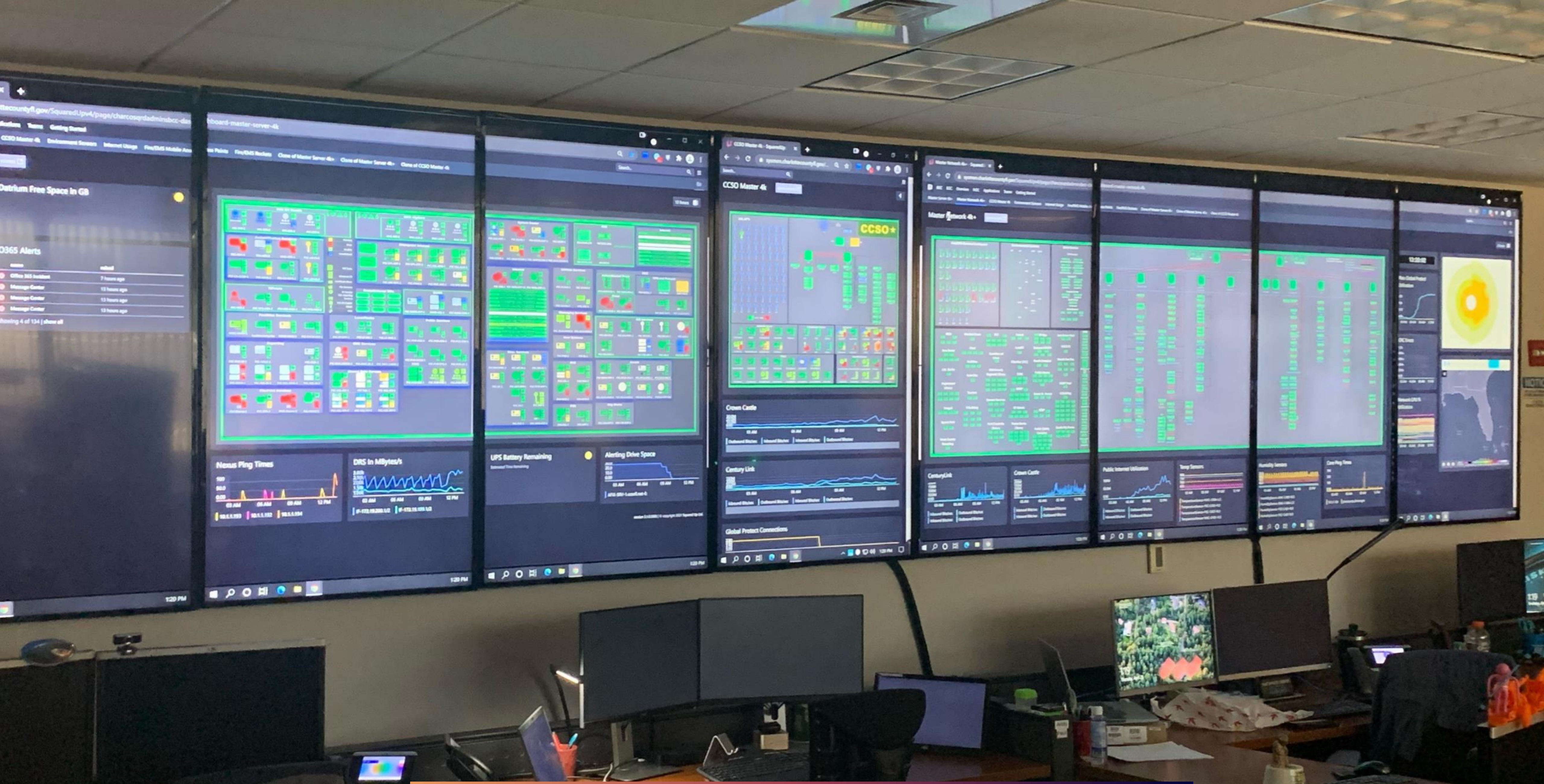
INTRODUCTION

36 Years in the IT Field

- 16 years with Charlotte County
  - Helpdesk Supervisor
  - Operations Manager
  - Sr Division Manager
- Past President – FLGISA
- Testified before Florida Cybersecurity Task Force Dec 2019
- Manatee County
  - Systems Analyst
  - Security Analyst
- Bridgewater State University (College)
  - Systems Manager
- Mass General Hospital
  - Computer Operator



DEC PDP-15 – MASS GENERAL HOSPITAL CIRCA 1985



CHARLOTTE COUNTY NETWORK OPERATIONS CENTER (NOC)

CURRENT STATE

LANDSCAPE

CURRENT STATE

LANDSCAPE

- Cyberattack Forces a Shutdown of a Top U.S. Pipeline

CURRENT STATE

LANDSCAPE

- Cyberattack Forces a Shutdown of a Top U.S. Pipeline
- Chinese government hackers targeted Microsoft’s enterprise email software

CURRENT STATE

LANDSCAPE

- Cyberattack Forces a Shutdown of a Top U.S. Pipeline
- Chinese government hackers targeted Microsoft’s enterprise email software
- Unknown hackers attempted to raise levels of sodium hydroxide in the water supply of Florida city

CURRENT STATE

LANDSCAPE

- Cyberattack Forces a Shutdown of a Top U.S. Pipeline
- Chinese government hackers targeted Microsoft’s enterprise email software
- Unknown hackers attempted to raise levels of sodium hydroxide in the water supply of Florida city
- Solarwinds – Software Supply-Chain

CURRENT STATE

LANDSCAPE

- Cyberattack Forces a Shutdown of a Top U.S. Pipeline
- Chinese government hackers targeted Microsoft’s enterprise email software
- Unknown hackers attempted to raise levels of sodium hydroxide in the water supply of Florida city
- Solarwinds – Software Supply-Chain
- The U.S. Department of Homeland Security revealed that hackers targeted the U.S. Census Bureau

CURRENT STATE

LANDSCAPE

- Cyberattack Forces a Shutdown of a Top U.S. Pipeline
- Chinese government hackers targeted Microsoft's enterprise email software
- Unknown hackers attempted to raise levels of sodium hydroxide in the water supply of Florida city
- Solarwinds – Software Supply-Chain
- The U.S. Department of Homeland Security revealed that hackers targeted the U.S. Census Bureau
- American healthcare firm Universal Health Systems sustained a ransomware attack

CURRENT STATE

LANDSCAPE

- Cyberattack Forces a Shutdown of a Top U.S. Pipeline
- Chinese government hackers targeted Microsoft’s enterprise email software
- Unknown hackers attempted to raise levels of sodium hydroxide in the water supply of Florida city
- Solarwinds – Software Supply-Chain
- The U.S. Department of Homeland Security revealed that hackers targeted the U.S. Census Bureau
- American healthcare firm Universal Health Systems sustained a ransomware attack
- Hackers threaten to release police records, knock 911 offline – Washington DC

CURRENT STATE

LANDSCAPE

- Cyberattack Forces a Shutdown of a Top U.S. Pipeline
- Chinese government hackers targeted Microsoft’s enterprise email software
- Unknown hackers attempted to raise levels of sodium hydroxide in the water supply of Florida city
- Solarwinds – Software Supply-Chain
- The U.S. Department of Homeland Security revealed that hackers targeted the U.S. Census Bureau
- American healthcare firm Universal Health Systems sustained a ransomware attack
- Hackers threaten to release police records, knock 911 offline – Washington DC
- Metropolitan Transportation Authority attacked by suspected Chinese hackers – NY
- JBS – Meat distributor - Ransomware

TYPES OF CYBER ATTACKS

- Ransomware and Extortion
- Theft of PII/PHI
- Business Email Compromise (BEC)
- Fraud
- DDOS
- Doxing
- Website Defacements
- Theft of IP

CURRENT STATE

COMMON TACTICS

- Phishing/Spear-Phishing
- Watering-hole Domains
- Credential Gathering
- Open Source and Network Reconnaissance
- Host-based exploitation
- Targeting Industrial Control Systems (SCADA)
- Supply Chain Compromise

CURRENT STATE

COVID-19

Bizjournals.com: "Cyberattacks on the rise during the Covid-19 pandemic"
•***Government Technology***: "How Is Covid-19 Creating Data Breaches?"
•***BBC***: "Coronavirus: How the world of work may change forever"
•***Interpol.int***: "INTERPOL report shows alarming rate of cyberattacks during COVID-19"
•***Techxplore.com***: "Ransomware surge imperils hospitals as pandemic intensifies"
•***PR Newswire***: "Top Cyber Security Experts Report: 4,000 Cyber Attacks a Day Since COVID-19 Pandemic"
•***ZDNet***: "COVID-19 pandemic delivers extraordinary array of cybersecurity challenges"

Govtech.com

CURRENT STATE

LOCAL GOVERNMENT LANDSCAPE

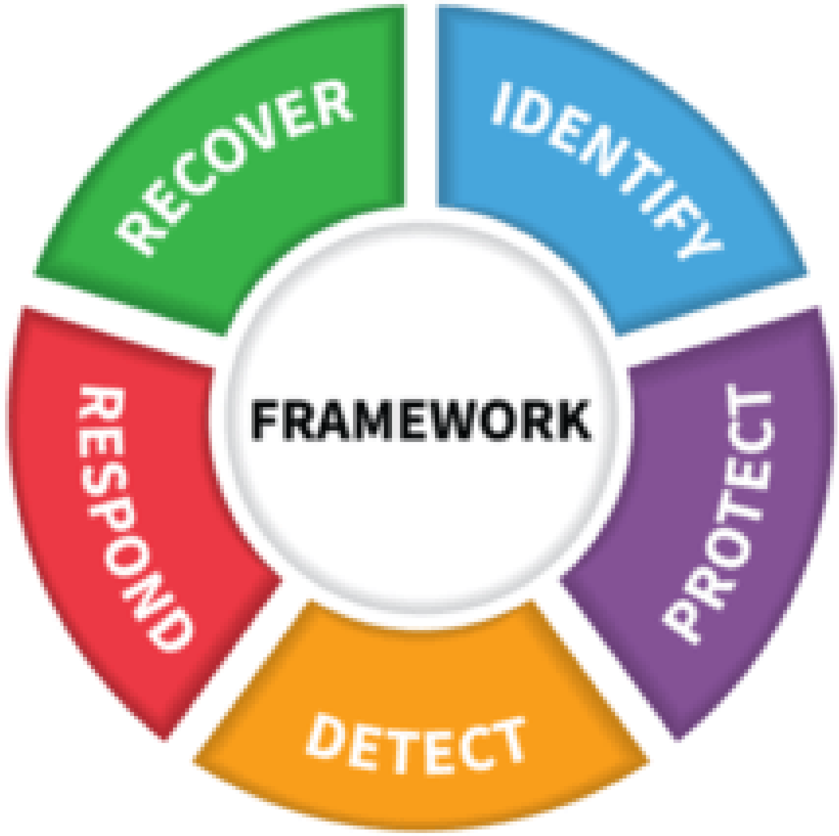
- Three-fourths of ransomware attacks in Florida over the last 3 years targeted public sector*
  - 78%, involve a local-government victim.*
- Several cases of government vendors being hit, Tyler, BillTrust, Superion, Solarwinds
- Ransomware Attack Affects Computers In 22 Towns In Texas ...
- Oldsmar Water Plant
- Ohio County Computer System Recovers from Malware Attack
- In 2020, at least 2,500 U.S. government entities, health care facilities and schools were victimized by ransomware. (Emsisoft)

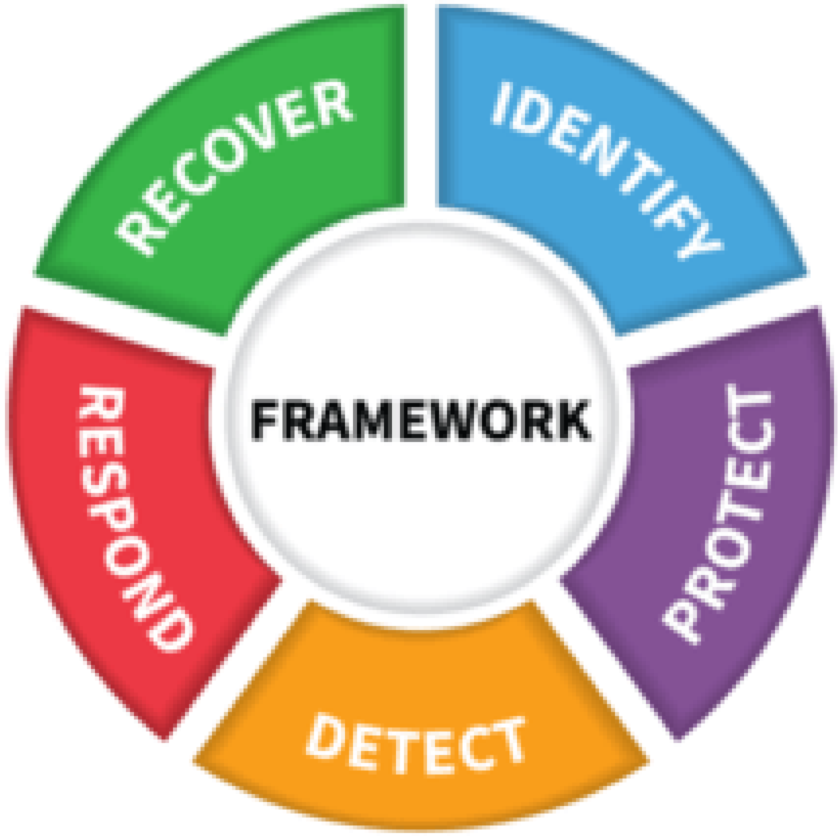
**https://statescoop.com/florida-ransomware-public-sector/*

CHALLENGES

- Limited budgets/Lack of funding
- Lack of IT expertise
- Insufficient cyber awareness
- PII/PHI
- PCI
- Executive buy-in/support
- Culture – convenience & easy access vs security
- More Than Just Monetary Damage - corrupting databases, erasing critical files and wreaking havoc on municipal networks, exfiltration/release of data
  - Reputation

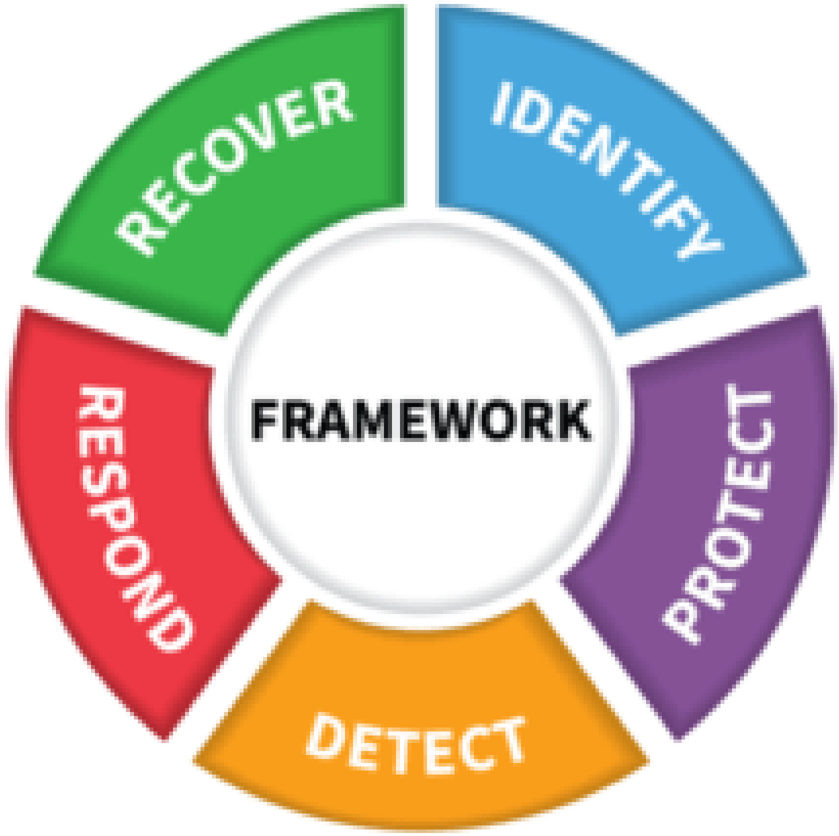
STEPS TO TAKE





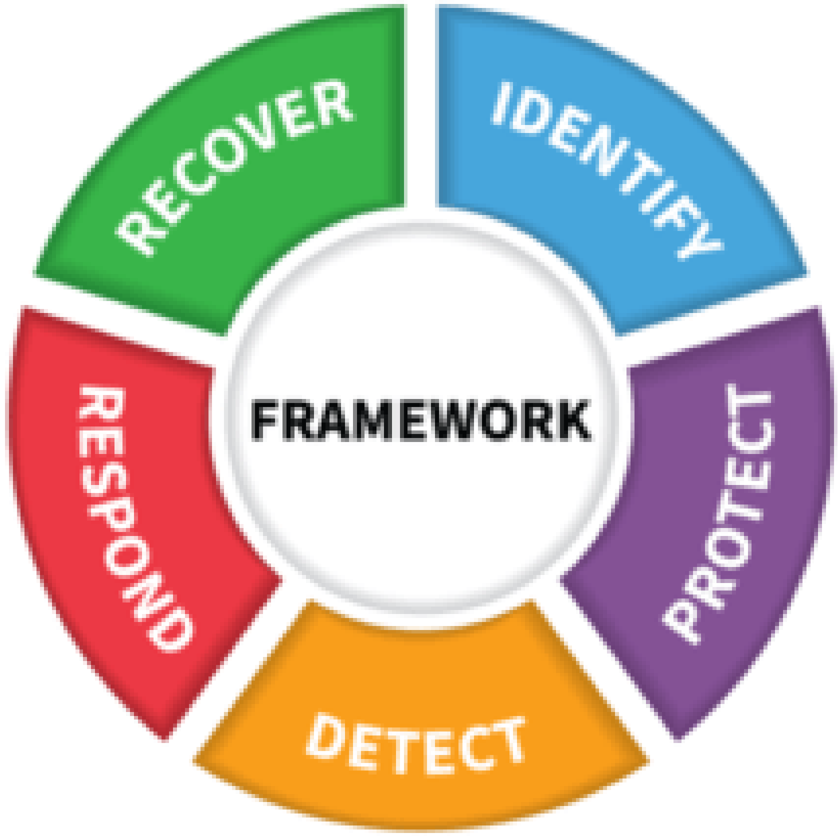
STEPS TO TAKE

- Identify, Protect, Detect, Respond, Recover



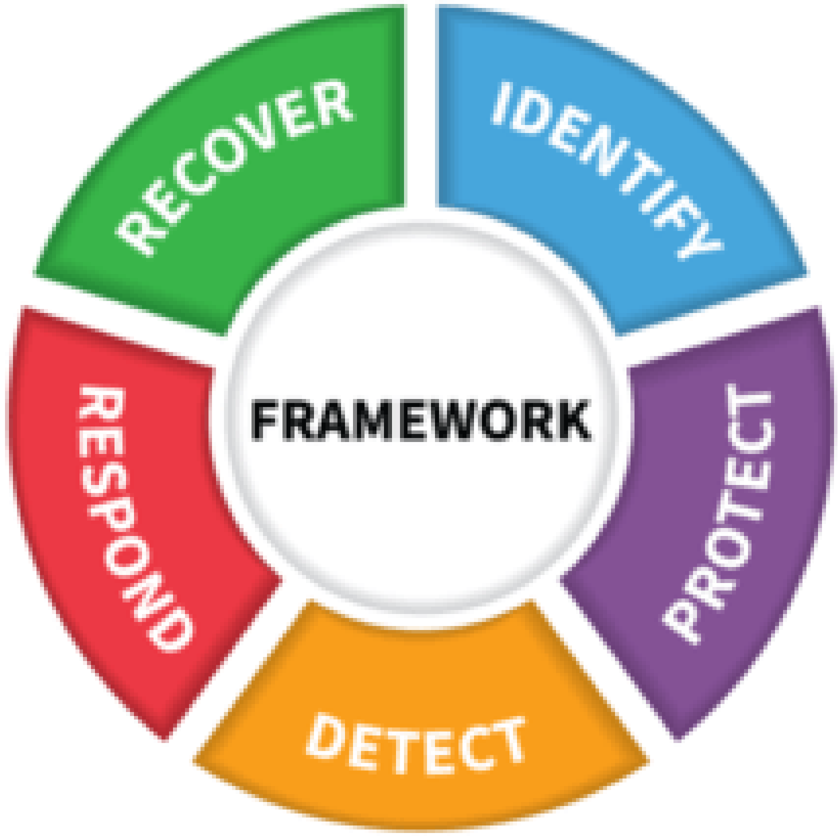
STEPS TO TAKE

- Identify, Protect, Detect, Respond, Recover
- Cyber Security Basics
  - Lock your car – patching, stay up to date, password policy, etc…



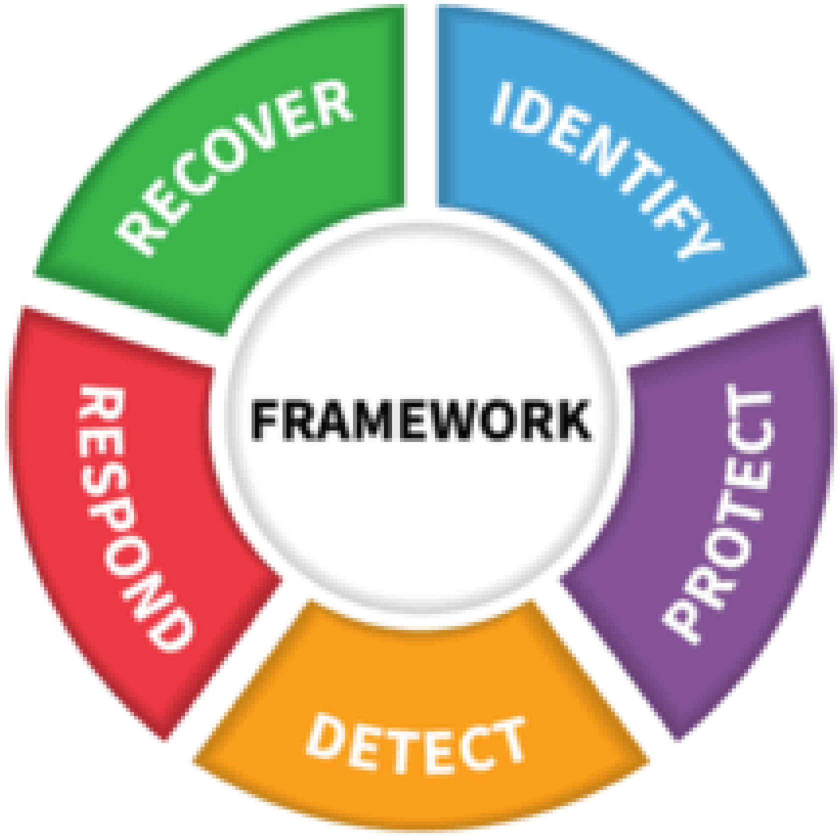
STEPS TO TAKE

- Identify, Protect, Detect, Respond, Recover
- Cyber Security Basics
  - Lock your car – patching, stay up to date, password policy, etc…
- MFA – Multi-Factor Authentication



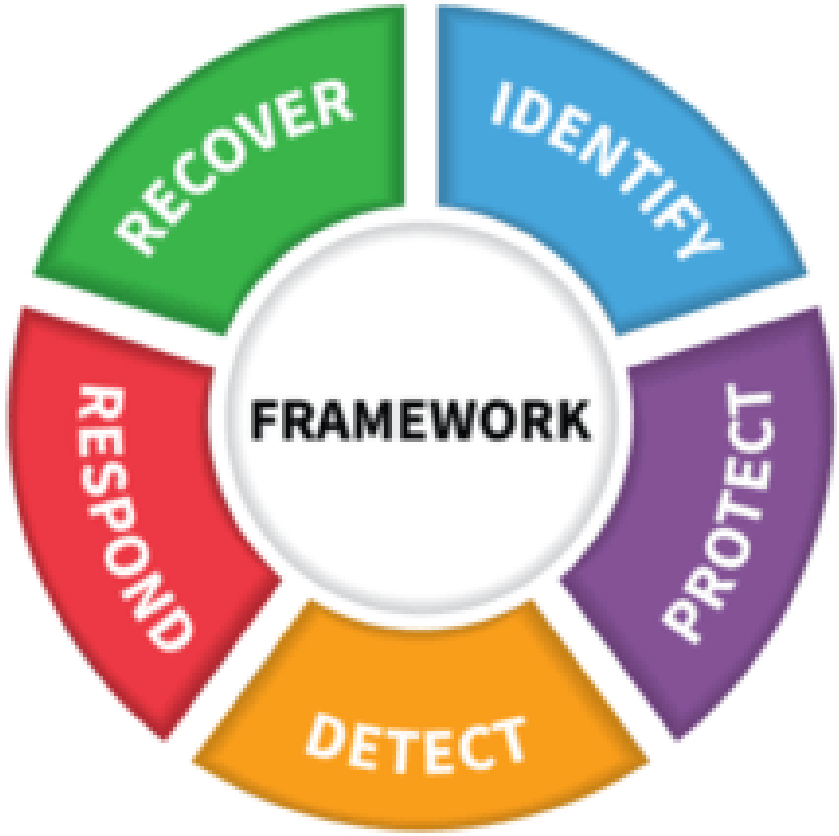
STEPS TO TAKE

- Identify, Protect, Detect, Respond, Recover
- Cyber Security Basics
  - Lock your car – patching, stay up to date, password policy, etc…
- MFA – Multi-Factor Authentication
- Data Backup – offline & tested



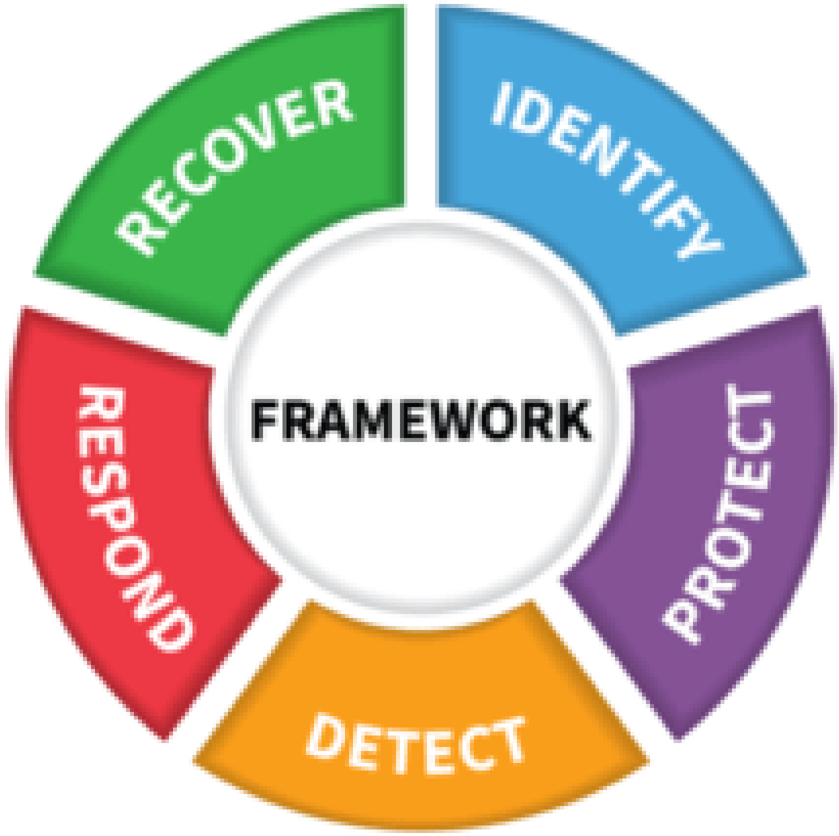
STEPS TO TAKE

- Identify, Protect, Detect, Respond, Recover
- Cyber Security Basics
  - Lock your car – patching, stay up to date, password policy, etc…
- MFA – Multi-Factor Authentication
- Data Backup – offline & tested
- Managed Security Services if inadequate IT Staff
  - Hybrid



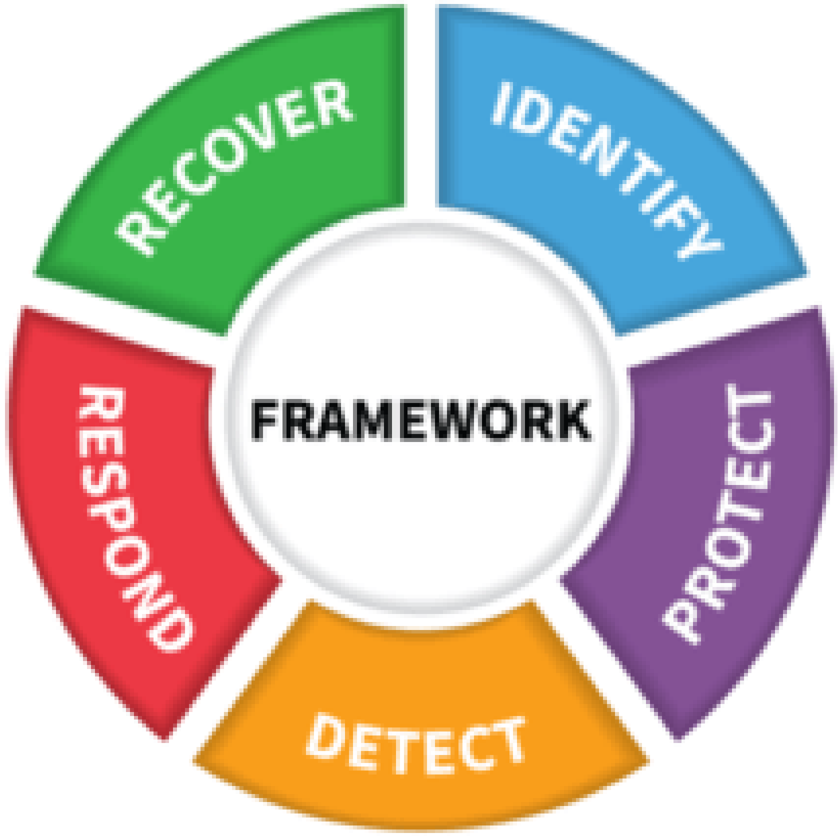
STEPS TO TAKE

- Identify, Protect, Detect, Respond, Recover
- Cyber Security Basics
  - Lock your car – patching, stay up to date, password policy, etc…
- MFA – Multi-Factor Authentication
- Data Backup – offline & tested
- Managed Security Services if inadequate IT Staff
  - Hybrid
- Regular Risk Assessments & cyber exercises



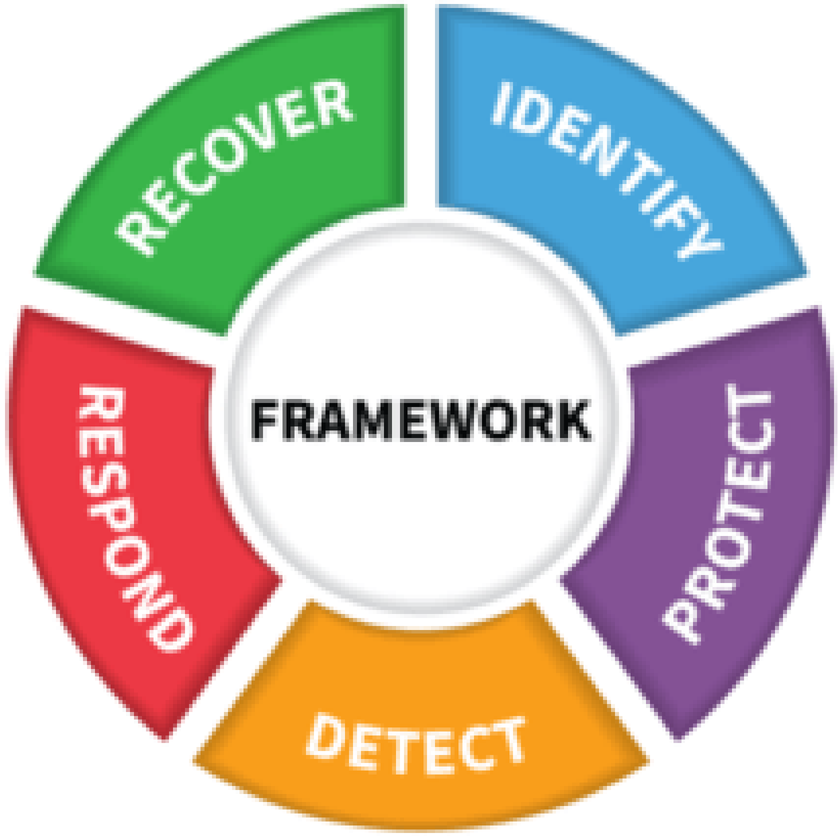
STEPS TO TAKE

- Identify, Protect, Detect, Respond, Recover
- Cyber Security Basics
  - Lock your car – patching, stay up to date, password policy, etc…
- MFA – Multi-Factor Authentication
- Data Backup – offline & tested
- Managed Security Services if inadequate IT Staff
  - Hybrid
- Regular Risk Assessments & cyber exercises
- Monitor - Internally and stay abreast



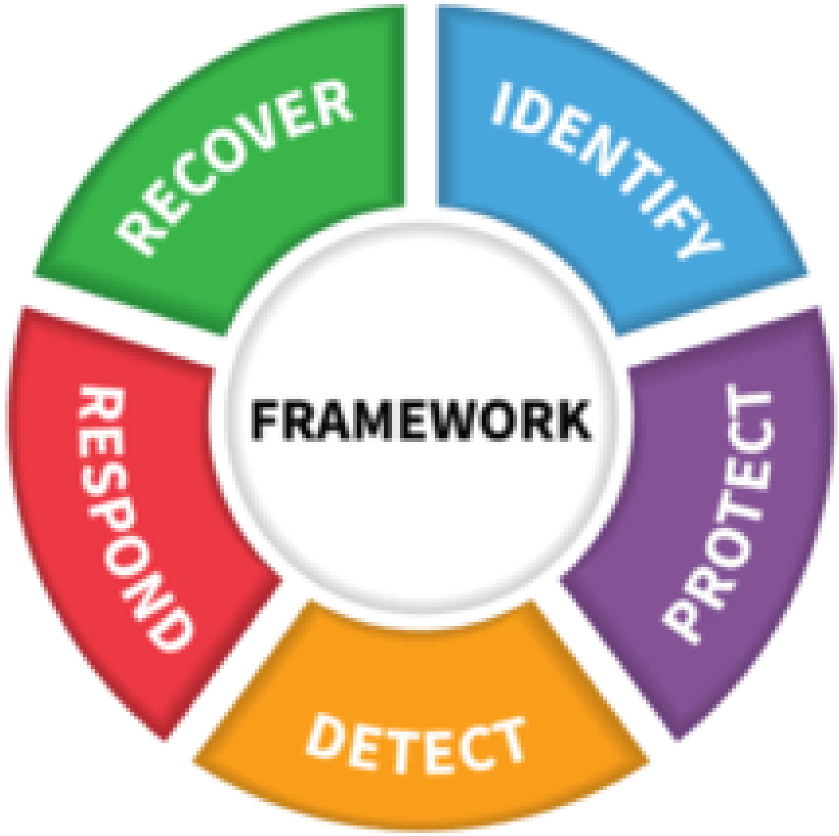
STEPS TO TAKE

- Identify, Protect, Detect, Respond, Recover
- Cyber Security Basics
  - Lock your car – patching, stay up to date, password policy, etc…
- MFA – Multi-Factor Authentication
- Data Backup – offline & tested
- Managed Security Services if inadequate IT Staff
  - Hybrid
- Regular Risk Assessments & cyber exercises
- Monitor - Internally and stay abreast
- Incident Response Plan
  - Organization wide involvement
    - Admin, Legal, HR, PIO, IT



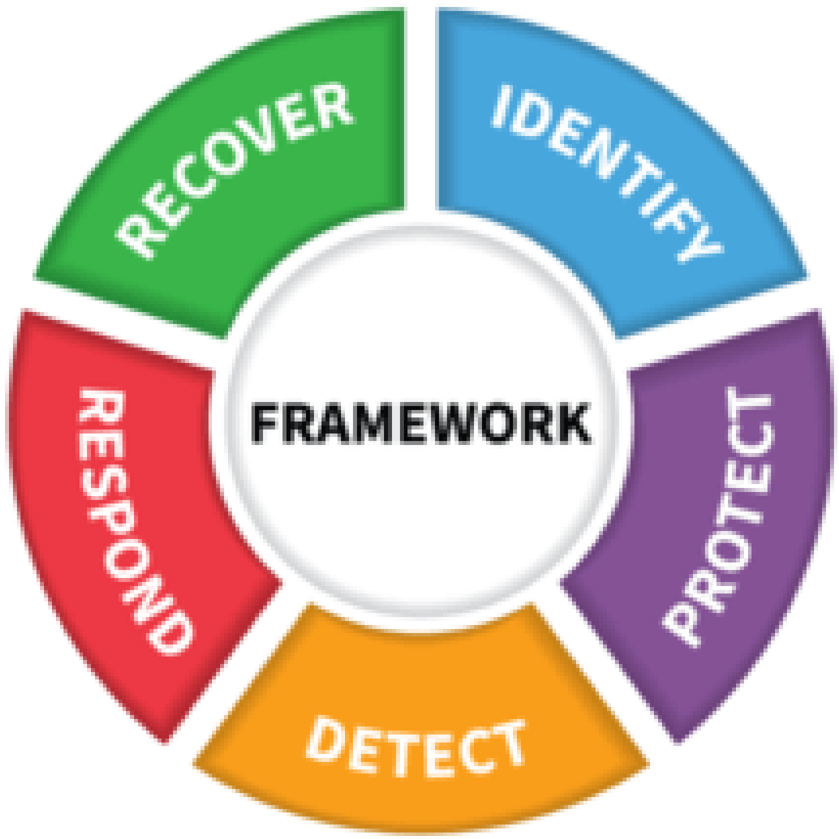
STEPS TO TAKE

- Identify, Protect, Detect, Respond, Recover
- Cyber Security Basics
  - Lock your car – patching, stay up to date, password policy, etc…
- MFA – Multi-Factor Authentication
- Data Backup – offline & tested
- Managed Security Services if inadequate IT Staff
  - Hybrid
- Regular Risk Assessments & cyber exercises
- Monitor - Internally and stay abreast
- Incident Response Plan
  - Organization wide involvement
    - Admin, Legal, HR, PIO, IT
- Clear Separation between Network Components
  - Network Segmentation



STEPS TO TAKE

- Identify, Protect, Detect, Respond, Recover
- Cyber Security Basics
  - Lock your car – patching, stay up to date, password policy, etc…
- MFA – Multi-Factor Authentication
- Data Backup – offline & tested
- Managed Security Services if inadequate IT Staff
  - Hybrid
- Regular Risk Assessments & cyber exercises
- Monitor - Internally and stay abreast
- Incident Response Plan
  - Organization wide involvement
    - Admin, Legal, HR, PIO, IT
- Clear Separation between Network Components
  - Network Segmentation
- Cyber Liability Insurance

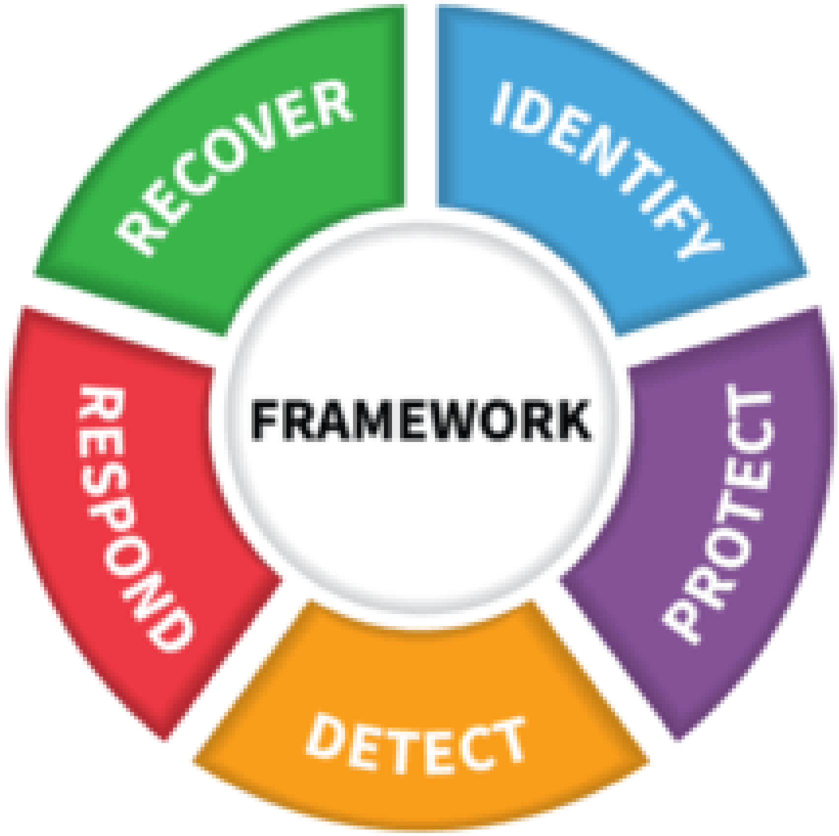


STEPS TO TAKE

- Identify, Protect, Detect, Respond, Recover
- Cyber Security Basics
  - Lock your car – patching, stay up to date, password policy, etc…
- MFA – Multi-Factor Authentication
- Data Backup – offline & tested
- Managed Security Services if inadequate IT Staff
  - Hybrid
- Regular Risk Assessments & cyber exercises
- Monitor – Internally and stay abreast
- Incident Response Plan
  - Organization wide involvement
    - Admin, Legal, HR, PIO, IT
- Clear Separation between Network Components
  - Network Segmentation
- Cyber Liability Insurance
  - But…Cyber insurance giant CNA hit by ransomware attack

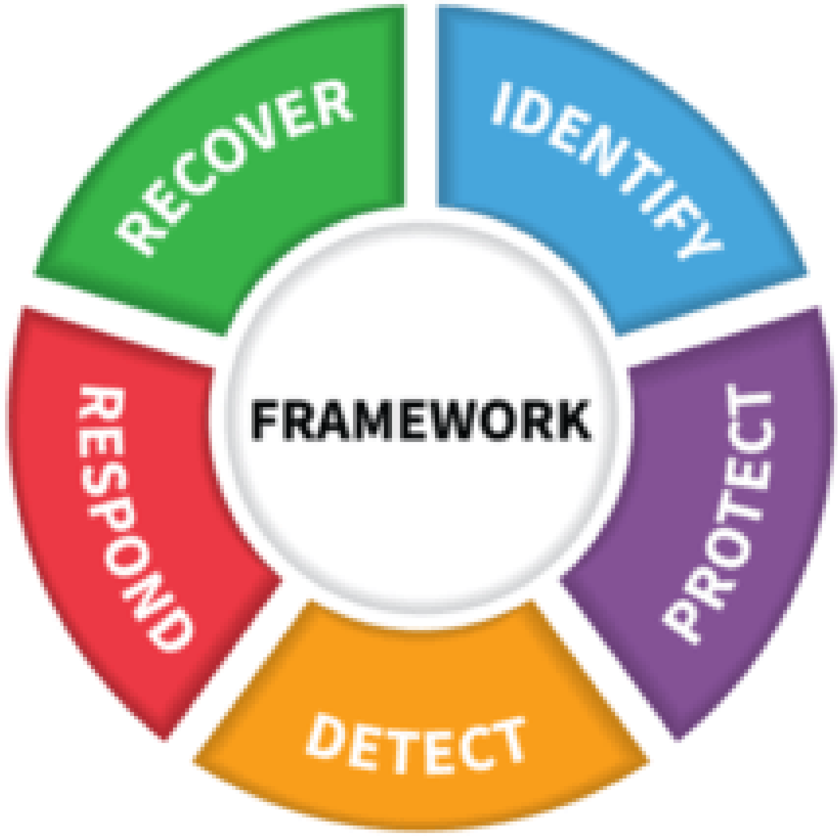
STEPS TO TAKE

- Identify, Protect, Detect, Respond, Recover
- Cyber Security Basics
  - Lock your car – patching, stay up to date, password policy, etc…
- MFA – Multi-Factor Authentication
- Data Backup – offline & tested
- Managed Security Services if inadequate IT Staff
  - Hybrid
- Regular Risk Assessments & cyber exercises
- Monitor - Internally and stay abreast
- Incident Response Plan
  - Organization wide involvement
    - Admin, Legal, HR, PIO, IT
- Clear Separation between Network Components
  - Network Segmentation
- Cyber Liability Insurance
  - But…Cyber insurance giant CNA hit by ransomware attack



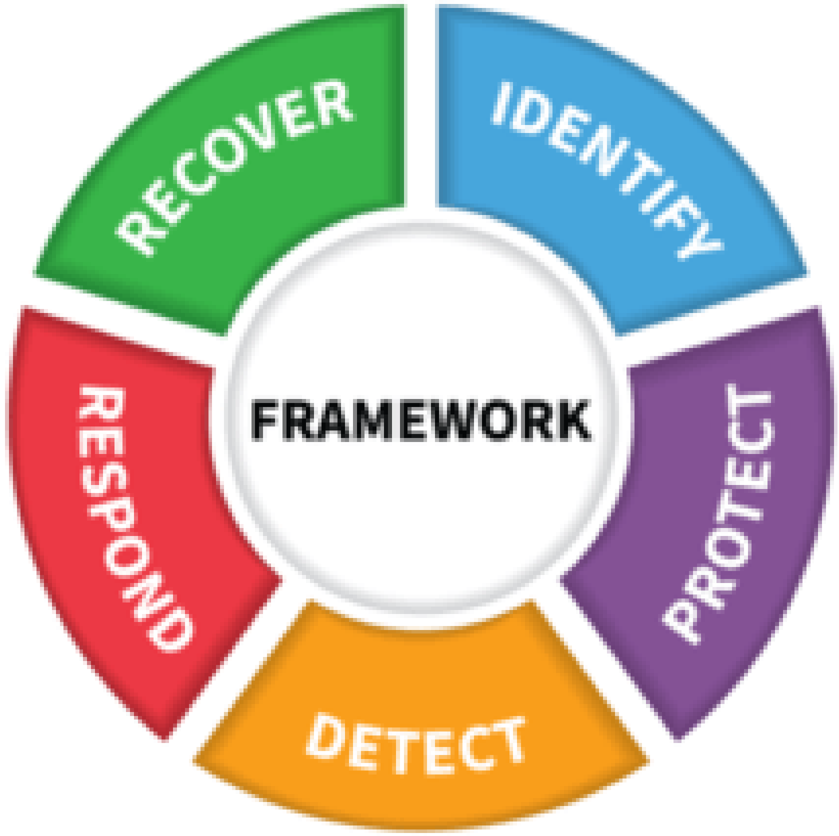
STEPS TO TAKE

- Identify, Protect, Detect, Respond, Recover
- Cyber Security Basics
  - Lock your car – patching, stay up to date, password policy, etc…
- MFA – Multi-Factor Authentication
- Data Backup – offline & tested
- Managed Security Services if inadequate IT Staff
  - Hybrid
- Regular Risk Assessments & cyber exercises
- Monitor - Internally and stay abreast
- Incident Response Plan
  - Organization wide involvement
    - Admin, Legal, HR, PIO, IT
- Clear Separation between Network Components
  - Network Segmentation
- Cyber Liability Insurance
  - But…Cyber insurance giant CNA hit by ransomware attack
- .Gov domain



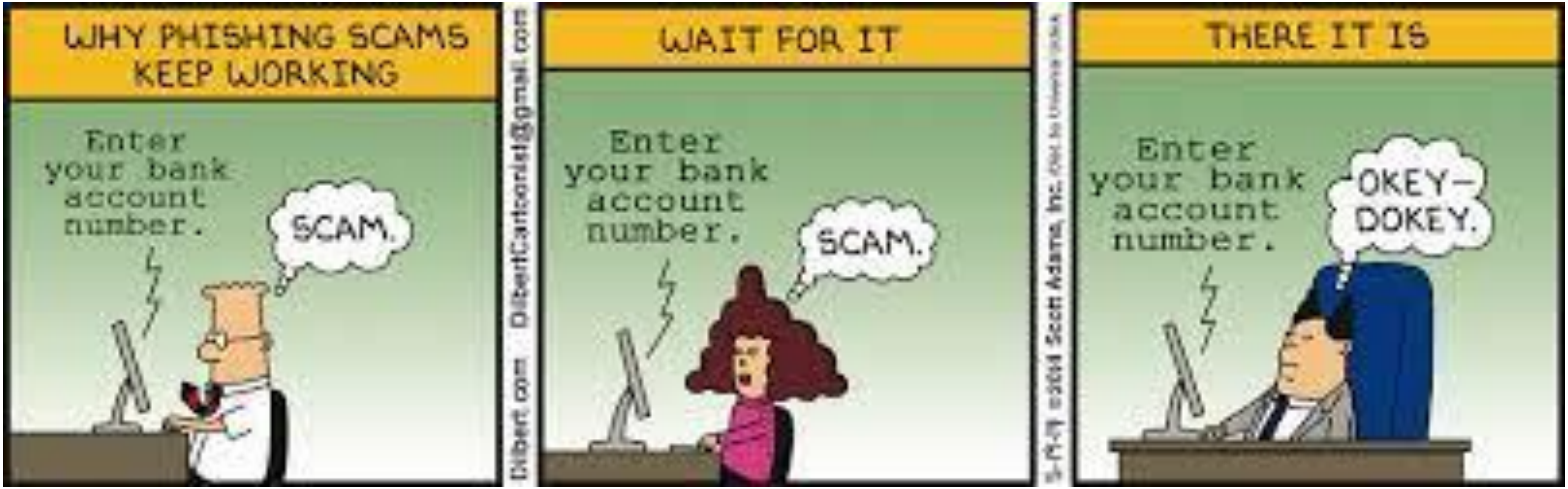
STEPS TO TAKE

- Identify, Protect, Detect, Respond, Recover
- Cyber Security Basics
  - Lock your car – patching, stay up to date, password policy, etc…
- MFA – Multi-Factor Authentication
- Data Backup – offline & tested
- Managed Security Services if inadequate IT Staff
  - Hybrid
- Regular Risk Assessments & cyber exercises
- Monitor - Internally and stay abreast
- Incident Response Plan
  - Organization wide involvement
    - Admin, Legal, HR, PIO, IT
- Clear Separation between Network Components
  - Network Segmentation
- Cyber Liability Insurance
  - But…Cyber insurance giant CNA hit by ransomware attack
- .Gov domain
- Defense in depth



WHAT ELSE IS NEEDED?

- State & Federal Funding/Grants
- Better Communication/Coordination between the state and local government
- Better response to cyber crime from Law Enforcement/Federal Government
- Certification of 3rd Part Providers (FedRamp/Stateramp)
- Educated Workforce



WHY PHISHING SCAMS KEEP WORKING
Enter your bank account number.
SCAM.
WAIT FOR IT
Enter your bank account number.
SCAM.
THERE IT IS
Enter your bank account number.
OKEY-DOKEY.

Dilbert.com DilbertCartoonist@gmail.com

© 2009 Scott Adams, Inc.

RESOURCES

- MS-ISAC/EI-ISAC/CIS
  - Multi State & Elections Infrastructure – Information Sharing & Analysis Center
    - https://ms-isac.org https://ei-isac.org

RESOURCES

- MS-ISAC/EI-ISAC/CIS
  - Multi State & Elections Infrastructure – Information Sharing & Analysis Center
    - https://ms-isac.org https://ei-isac.org

- CISA - Cybersecurity & Infrastructure Security Agency - DHS – https://CISA.org

RESOURCES

- MS-ISAC/EI-ISAC/CIS
  - Multi State & Elections Infrastructure – Information Sharing & Analysis Center
    - https://ms-isac.org https://ei-isac.org

- CISA - Cybersecurity & Infrastructure Security Agency - DHS – https://CISA.org

- FLGISA – Florida Local Government Information Systems Association – https://FLGISA.org

RESOURCES

- MS-ISAC/EI-ISAC/CIS
  - Multi State & Elections Infrastructure – Information Sharing & Analysis Center
    - https://ms-isac.org https://ei-isac.org
- CISA - Cybersecurity & Infrastructure Security Agency - DHS – https://CISA.org
- FLGISA – Florida Local Government Information Systems Association – https://FLGISA.org
- NACo – https://Naco.org
  - NACo Cyber Security Priorities and Best Practices

RESOURCES

- MS-ISAC/EI-ISAC/CIS
  - Multi State & Elections Infrastructure – Information Sharing & Analysis Center
    - https://ms-isac.org https://ei-isac.org
- CISA - Cybersecurity & Infrastructure Security Agency - DHS – https://CISA.org
- FLGISA – Florida Local Government Information Systems Association – https://FLGISA.org
- NACo – https://Naco.org
  - NACo Cyber Security Priorities and Best Practices
- FBI InfraGard - https://www.infragard.org/

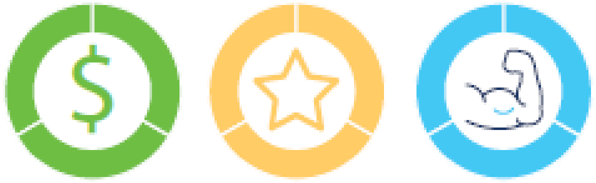
RESOURCES

- MS-ISAC/EI-ISAC/CIS
    - Multi State & Elections Infrastructure – Information Sharing & Analysis Center
        - https://ms-isac.org https://ei-isac.org
- CISA - Cybersecurity & Infrastructure Security Agency - DHS – https://CISA.org
- FLGISA – Florida Local Government Information Systems Association – https://FLGISA.org
- NACo – https://Naco.org
    - NACo Cyber Security Priorities and Best Practices
- FBI InfraGard - https://www.infragard.org/
- SANS Institute - https://isc.sans.edu/ https://www.sans.org/

$ **Cost** ☆ **Cyber Defense Impact** **Workload Effort**

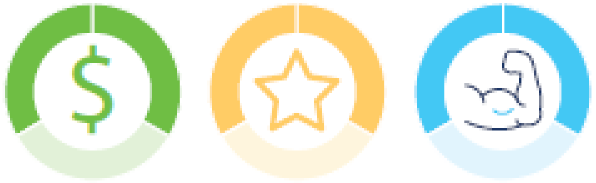
The icons represent the percentage of cost, impact on cyber defenses and workload effort needed to implement the priority. The more complete the outer circle of the icon is, the higher the percentage of cost, impact or workload, but also is dependent on current county circumstances.

MFA (Multi-Factor Authentication)



It is a proven fact that multi-factor authentication significantly decreases the amount of successful cyber-attacks on a county. Depending on the main technology platform that a county has implemented for end user authentication, will determine the cost, as well as time and resources needed. And let us not forget the education with end users. MFA solutions alone can run into hundreds of thousands of dollars, depending on the size of the county.

DMARC (Domain-based Message Authentication, Reporting and Conformance)



DMARC is an email authentication protocol. The percentage of local government implementing this security feature is on the low side. The main cost associated with DMARC is hiring the resource to handle implementation of the feature on a county's existing infrastructure or training current IT staff to do so.

SUMMARY

- NOT A MATTER OF IF, BUT WHEN

SUMMARY

- NOT A MATTER OF IF, BUT WHEN
- NOT A MATTER OF JUST PREVENTION
  - Identify, Protect, Detect, Respond, Recover

SUMMARY

- NOT A MATTER OF IF, BUT WHEN
- NOT A MATTER OF JUST PREVENTION
  - Identify, Protect, Detect, Respond, Recover
- CAN'T GO IT ALONE
  - Take advantage of Resources available

SUMMARY

- NOT A MATTER OF IF, BUT WHEN
- NOT A MATTER OF JUST PREVENTION
  - Identify, Protect, Detect, Respond, Recover
- CAN'T GO IT ALONE
  - Take advantage of Resources available
- TAKES A VILLAGE
  - Not Just an IT Issue - Organizational

SUMMARY

- NOT A MATTER OF IF, BUT WHEN
- NOT A MATTER OF JUST PREVENTION
  - Identify, Protect, Detect, Respond, Recover
- CAN’T GO IT ALONE
  - Take advantage of Resources available
- TAKES A VILLAGE
  - Not Just an IT Issue - Organizational
- DEFENSE IN DEPTH

SUMMARY

- NOT A MATTER OF IF, BUT WHEN
- NOT A MATTER OF JUST PREVENTION
  - Identify, Protect, Detect, Respond, Recover
- CAN’T GO IT ALONE
  - Take advantage of Resources available
- TAKES A VILLAGE
  - Not Just an IT Issue - Organizational
- DEFENSE IN DEPTH
- MINIMIZE RISK
  - Reduce attack surface

THANK YOU

QUESTIONS?

Ray Desjardins, CGCIO

Ray.Desjardins@charlottecountyfl.gov

FLGISA.ORG