# Florida Department of State
# Cyber Navigator Program

# Christopher Krebs

Director of DHS CISA

July 11th, 2018

DHS'S PROGRESS IN SECURING ELECTION SYSTEMS AND OTHER CRITICAL INFRASTRUCTURE

There are things as simple as hiring what we are calling a *cyber navigator*, someone that actually has cybersecurity expertise that can get out from your State capital and go work with the various counties.

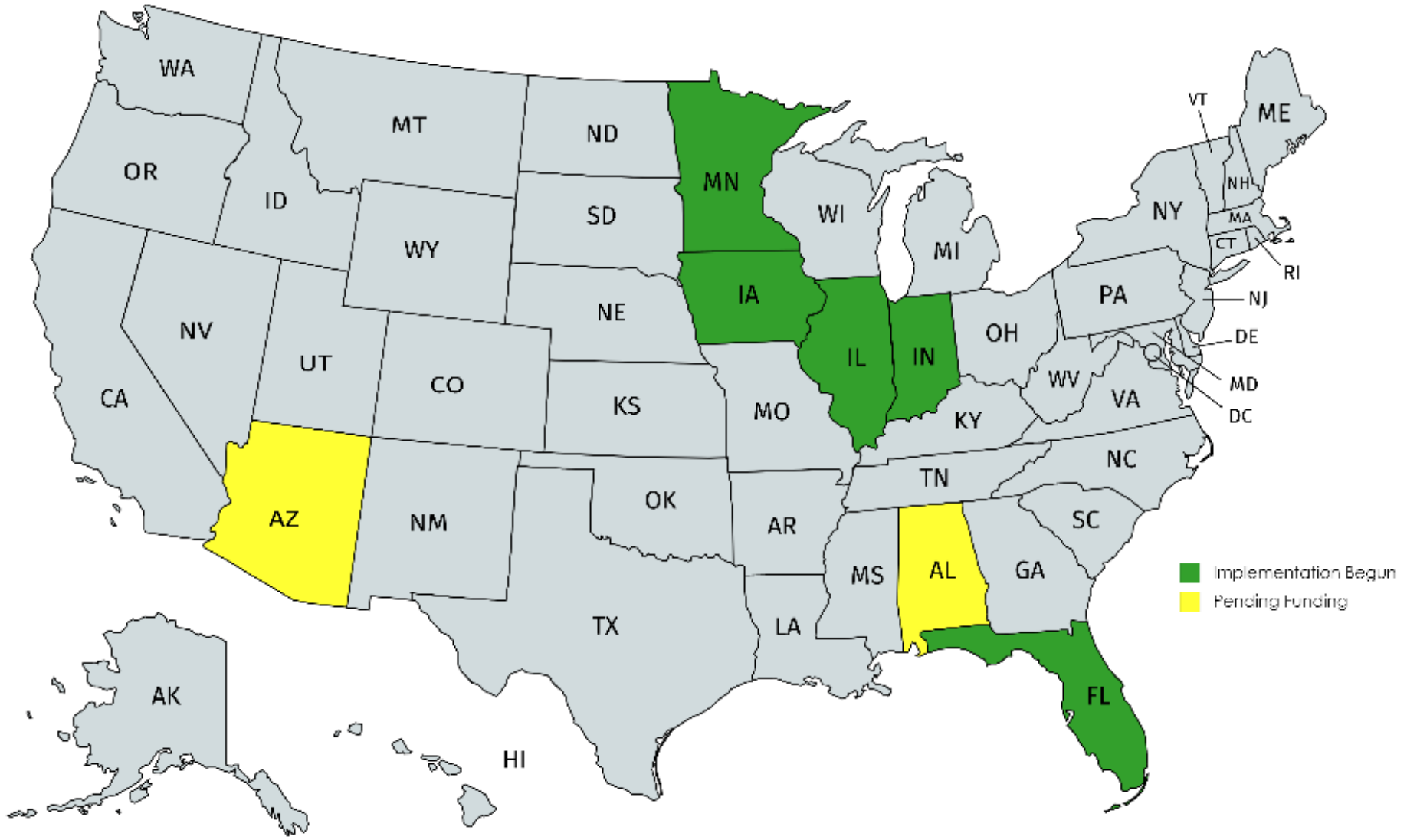
Because that is the real challenge here, is that when you think about across the Nation, there's close to, if not over, 10,000 jurisdictions and there's not enough cybersecurity expertise to go around as it stands, so let's--let's continue to invest in that.

# States with Cyber Navigator Programs

Multiple States have taken Homeland Security's recommendation and are beginning to implement cyber liaisons over the next few years.

**Pending Funding**

**Implementation Underway**



# The State of Florida Program

Created under then Governor Rick Scott in 2018 to provide cybersecurity subject matter expertise to local Elections Officials.

AP

Florida Gov. orders hiring of election security consultants

# Florida Gov. orders hiring of election security consultants

By GARY FINEOUT May 3, 2018

Click to copy

RELATED TOPICS

Legislature

Florida

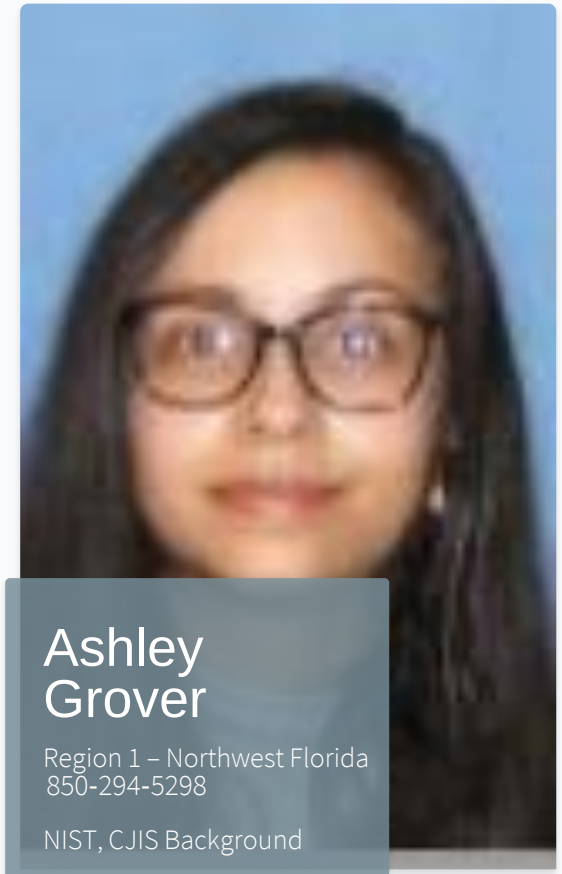
TALLAHASSEE, Fla. (AP) — Florida Gov. Rick Scott said Thursday that the state would hire special election security consultants in advance of this year's critical elections despite state legislators rejecting a similar request earlier this year.

Scott and state officials had asked the Florida Legislature to create a cybersecurity unit in the state's elections office to combat a "growing threat." The move came after an effort to infiltrate the state's election systems during the 2016 elections.

# Current Navigator Team

A collection of different experiences and backgrounds brought together for the benefit of Elections Offices.

**Cyber Navigator Hotline: 850-245-6502**

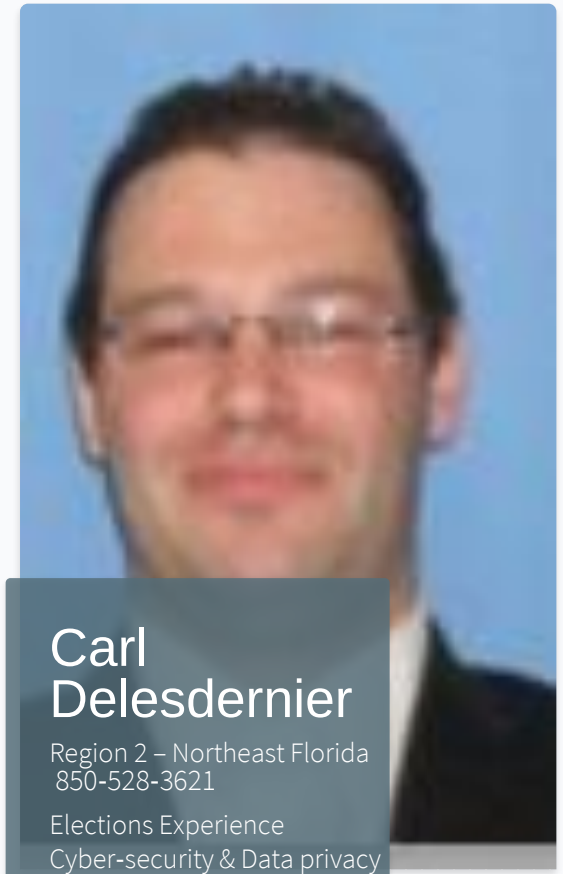


## Ashley Grover

Region 1 – Northwest Florida
850-294-5298

NIST, CJIS Background

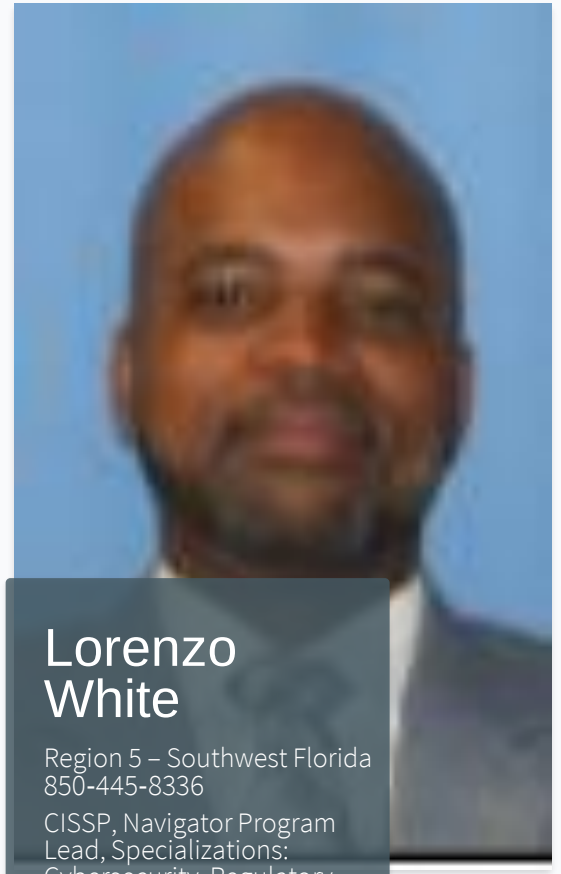
Threat intelligence, Policy Creation, End User Training



## Carl Delesdernier

Region 2 – Northeast Florida
850-528-3621

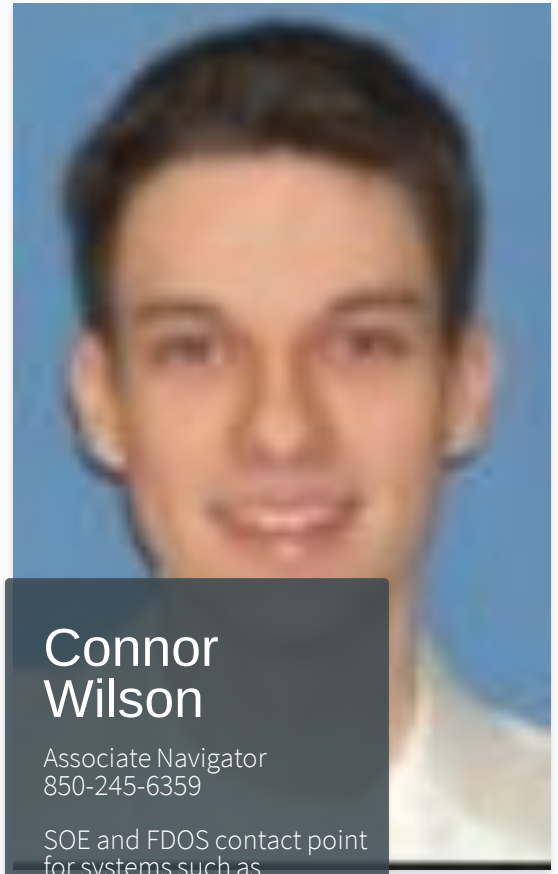
Elections Experience
Cyber-security & Data privacy
Incident Handling
Network Hardening



## Lorenzo White

Region 5 – Southwest Florida
850-445-8336

CISSP, Navigator Program Lead, Specializations: Cybersecurity, Regulatory Compliance, Incidence Response



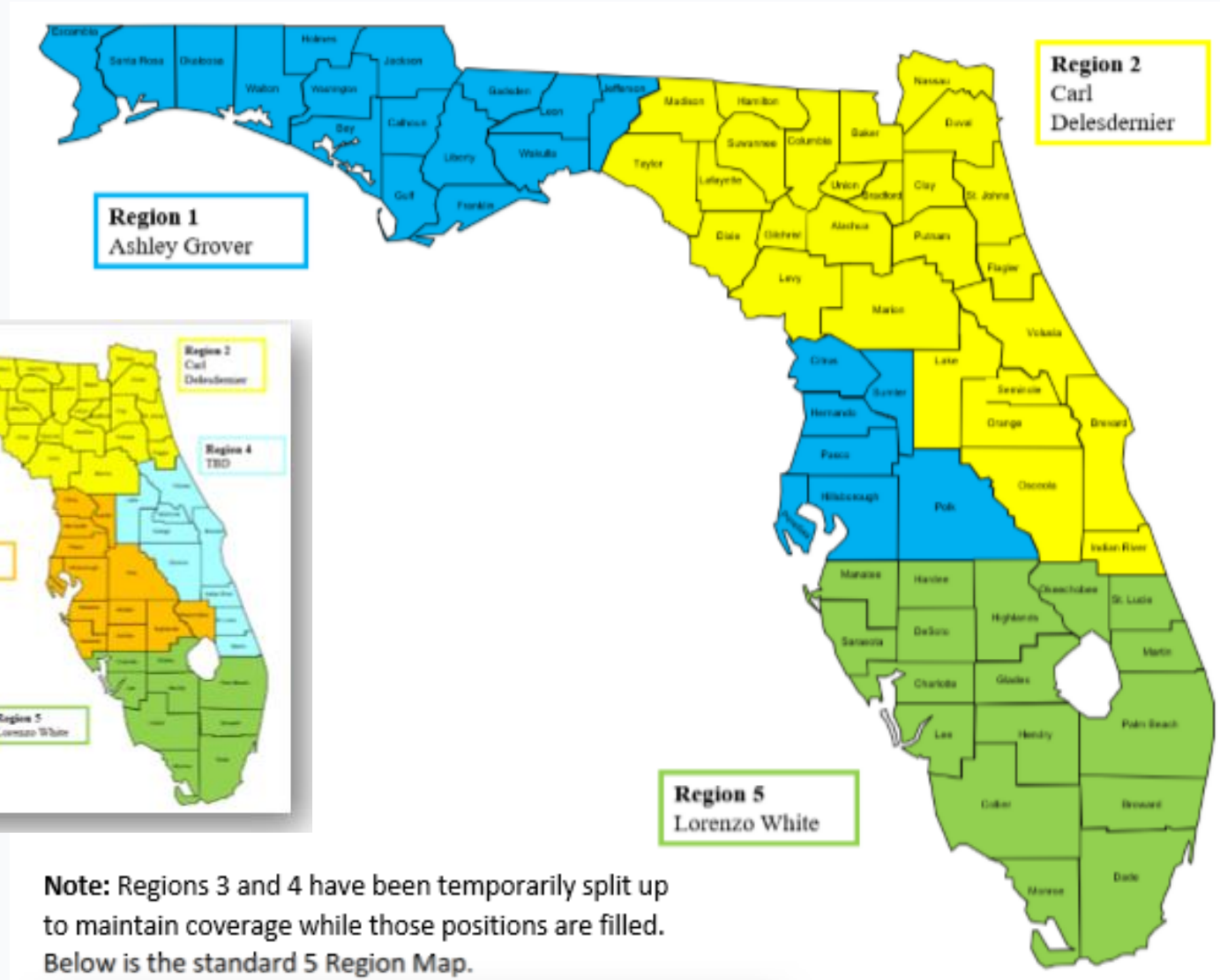
## Connor Wilson

Associate Navigator
850-245-6359

SOE and FDOS contact point for systems such as MIM\FVRS and some SOE Portal functions

# Regions

Each Navigator serves as the primary contact for a specific region.

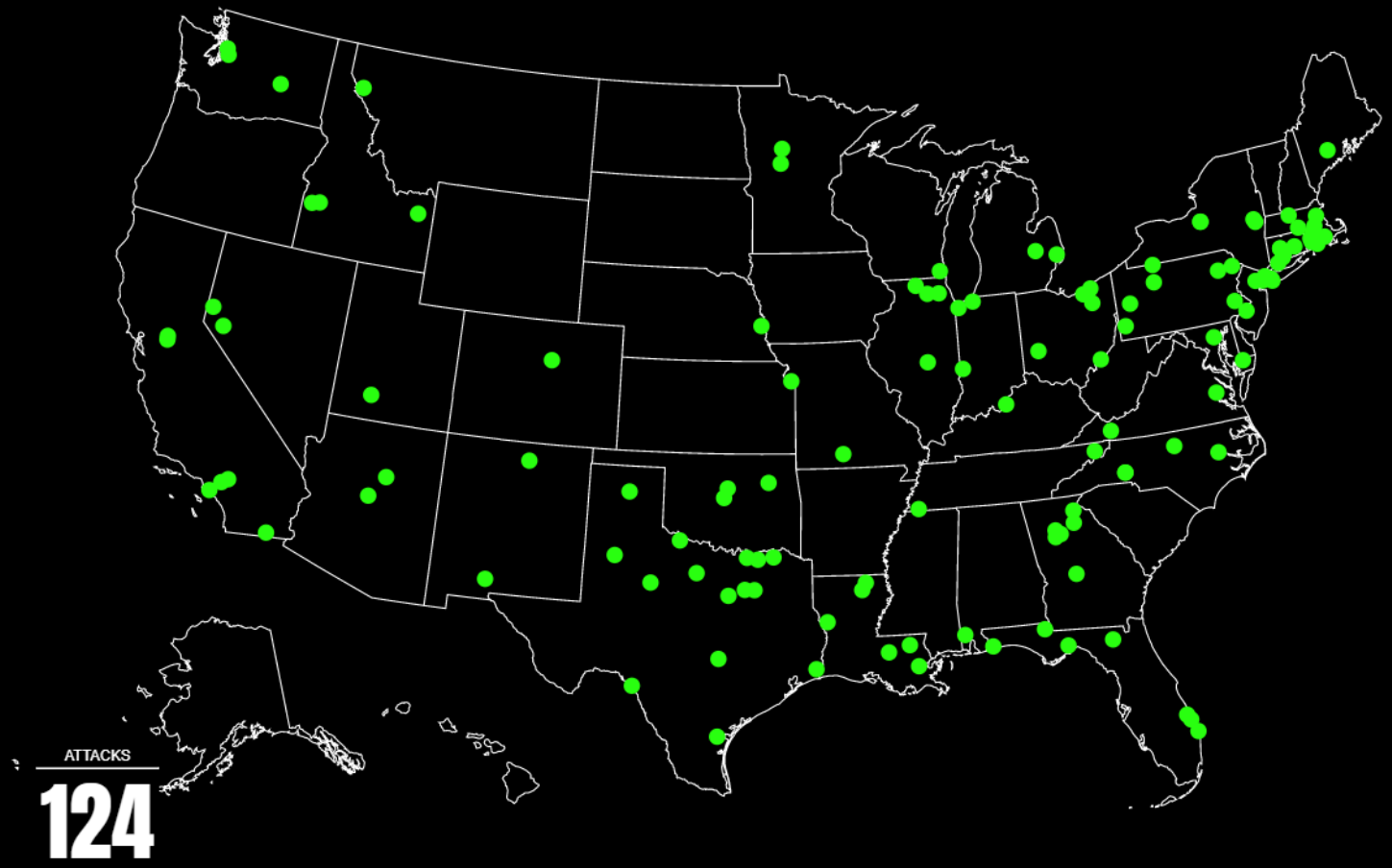




**Note:** Regions 3 and 4 have been temporarily split up to maintain coverage while those positions are filled. Below is the standard 5 Region Map.


file edit folder tools info help
img_134.jpg
img_1189.jp
img_6856.jpg
img_6856.jpg
RANSOMWARE ATTACK
PAY TO UNLOCK YOUR FILES

# Ransomware and Government IT

State and Local Government agencies have become a common target for ransomware campaigns, especially from those looking to capitalize on a lack of budget and cybersecurity training.




Reported Attacks Against State and Local Governments in 2019

https://statescoop.com/Ransomware-Map/

# RANSOMWARE'S RISE

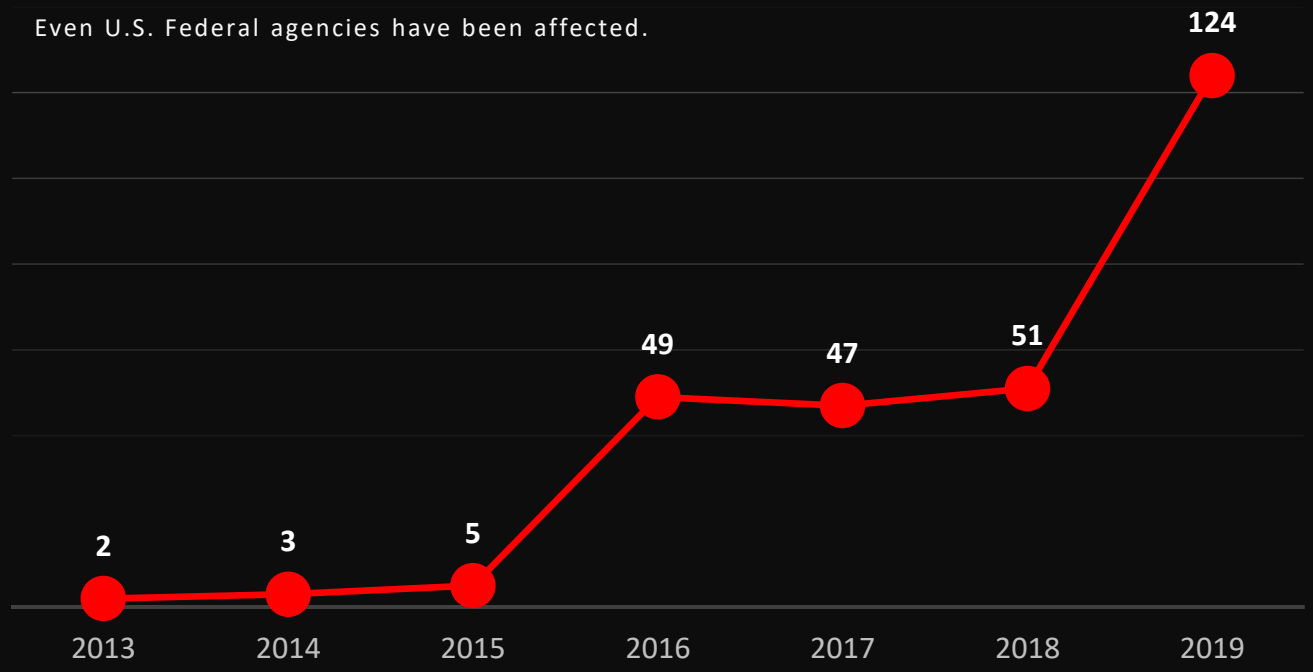
Ransomware is a recent development, and the scourge has really taken off over the past couple years. While we're only discussing ransomware's effect on state and local government, there is no industry that hasn't felt the pain of this infection. Other common and high-profile targets include hospitals and medial care providers, companies in the oil and gas industry, and utility companies. Even U.S. Federal agencies have been affected.

## Reported Attacks Per Year

According to data from Statescoop.com, reported attacks have skyrocketed in 2019 with over double the number of reported attacks against state and local government targets in 2019 than in 2018. This doesn't include unreported attacks that may never come to light.

## Bigger Ransoms

Attacks reported in 2013 and 2014 had small ransom demands, usually around $500. Ransom demands have gone up with the number of infections. For example, the August 2019 attack against the Vernon Texas Police Department included a **$2.5 million dollar ransom**.



# DO THEY PAY THE RANSOM?

Most agencies do not pay the attackers and work diligently towards restoring their systems post attack. However, some agencies do pay which spurs attackers on in the hopes of making more profits. The FBI and DHS state that ransoms should not be paid as it encourages more ransomware attacks. There's also new strains of ransomware that are simply extortion. The ransomware is completely destructive, and files cannot be recovered whether the ransom is paid or not.


**LAKE CITY, FL**

The city government of Lake City, FL paid a ransom of over $490,000 in 2019 to unlock emails and phone systems.

**RIVIERA BEACH, FL**

The city government of Riviera Beach, FL paid over $590,000 to attackers in 2019 after their network was shutdown.

# IN THE NEWS

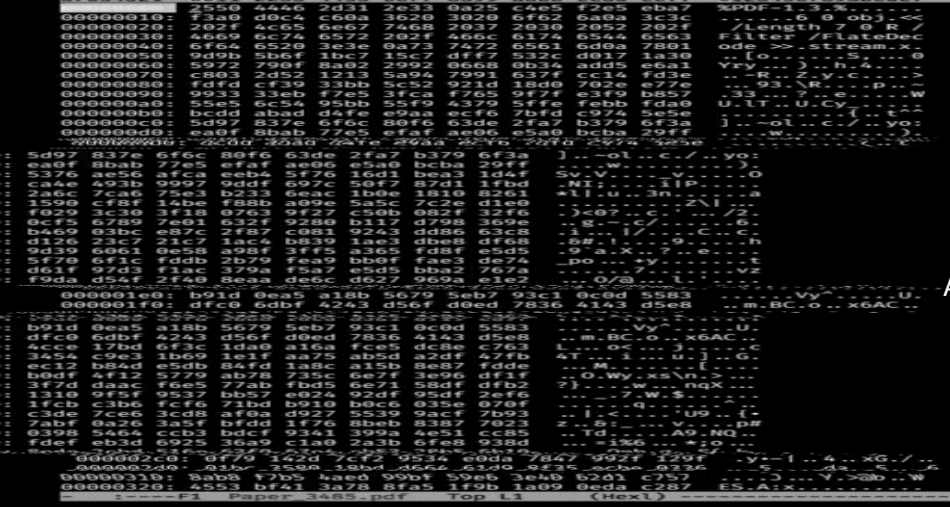
Attacks on large cities and government agencies make national headlines as potentially hundreds of thousands of citizens are impacted by service outages. Here's three famous examples of major attacks.


**2018** Colorado's Department of Transportation suffered a major outage after SamSam ransomware took down their network. The Governor declared a statewide emergency after the attack lasted 10 days and clean up efforts cost over **$1.5 million**.


**2018** The City of Atlanta cyberattack has been well studied as one of the largest ransomware attacks of all time with recovery costs potentially in excess of **$17 million** and effects felt by over **400,000** citizens.

Let's take a quick walkthrough of the Atlanta cyberattack.


**2019** Poor IT practices and a lack of funding result in Baltimore falling victim to the RobinHood ransomware. City functions such as property sales halted for weeks and the cleanup costs topped **$18 million**.



# SYSTEM OUTAGE

At 5:40 AM on March 28th, 2018 the City of Atlanta's Information Management Team receives alerts of an infection…

## BEFORE THE ATTACK

Multiple audits and assessments throughout 2017 and 2018 reveal over 2,000 vulnerabilities and misconfigured systems. Budget shortages and an IT culture that ignores best practice leaves these systems wide open for exploit.

## THE INFECTION

Attackers find these outdated servers exposed to the Internet and attack the weak passwords in order to gain access. Once inside, they start manually installing SamSam ransomware across the network.

## THE DAMAGE IS DONE

Residents begin losing access to services…

# ***OUTAGE ALERT***

**The City of Atlanta is currently experincing outages on various internal and customer facing applications, including some applications that customers use to pay bills or access court-related information. At this time, our Atlanta Information Management team is working diligently with support from Microsoft to reslove the issue. We are confident that our team of technology professionals will be able to restore applications soon. Our City website, Atlantaga.gov, remains accessible and we will provide updates as we receive them.**

ATL Municipal Court
@ATLCourt

**As the City of Atlanta vigorously works to resolve technical outages, Court dates scheduled for TODAY, March 29th will be reset. Please check your ticket and verify your mailing address is current to ensure you receive your reset notice in the mail.**

MUNICIPAL COURT OF ATLANTA

@atlantamunicipalcourt @ATLCourt @ATLCourt

# NATIONAL NEWS

Widespread outages leave hundreds of thousands of citizens unable to pay traffic tickets, access court information, pay bills, and more. The Mayor and city officials are forced to go before national news outlets to explain the situation.



The City calls in support from State, Federal, and private industry partners to control the infection and begin restoring services. The bill for recovery crests **$2.5 million** in days, and spirals to over **$17 million** by the time everything is said and done. Full restoration of services takes weeks.

# LOCAL NEWS


Ransomware attack on San Francisco public transit gives everyone a free ride

San Francisco Municipal Transport Agency attacked by hackers who locked up computers and data with 100 bitcoin demand

▲ Above ground it was business as usual but San Fransisco's Municipal Transport Agency fell victim to ransomware on Friday. Photograph: Robert Galbraith/REUTERS

**San Francisco MUNI - 2016**

San Francisco's Mass Transit Authority, MUNI, suffers a ransomware attack that leaves them unable to take payments resulting in free rides for all.


THE TEXAS TRIBUNE

23 Texas cities were targeted in a "coordinated ransomware attack"

The majority of attacks were against small local governments, according to the state's Department of Information Resources.

BY TROY CLOSSON AUG. 19, 2019 1 PM

**Texas - 2019**

A wave of ransomware attacks washed over Texas taking at least 23 city governments offline in less than a week's time.

**City of Albany, NY - 2019**

Police and other essential services were forced to work offline as City Information Technology team members worked to restore systems from offline backups as quickly as possible.


NEWS

TIMES UNION

Albany's repair cost after ransomware attack: $300,000

City officials say offline backup servers helped Albany avoid ransom payment

Amanda Fries | Sep. 27, 2019 | Updated: Sep. 27, 2019 3:18 p.m.

**State of Louisiana - 2019**

Public agencies were crippled by the Ryuk ransomware and motor vehicles offices were closed for over 2 weeks. Governor Jon Bel Edwards stated, "some, but not all state servers" were affected.


SECURITY

Some Offices Still Closed After Louisiana Ransomware Attack

*Nearly three-quarters of Louisiana's motor vehicle offices remained closed Monday as state workers continue to respond to the lingering effects of a cyberattack that hit state servers two weeks ago.*

BY SAM KARLIN, THE ADVOCATE / DECEMBER 3, 2019



Not every attack gets covered on national news such as CNN or Fox.
But more often than not, the news gets out. Even if it's just at the local level.
Here's some examples of news reports over the last few years highlighting just how widespread ransomware attacks truly are.

# PRACTICAL DEFENSE

Strong defenses will often prevent ransomware attacks from ever getting a foothold. While some agencies have started purchasing cyber insurance and advanced defense systems, there are some common and practical cyber hygiene precautions that any organization can take to minimize their chances of being a victim.

## USER TRAINING

**Users are often the first line of defense against attacks like ransomware. Training users not to open or run unknown files, programs, and mail attachments will prevent many attacks.**

## MAIL FILTER

**Most phishing messages are connected to ransomware campaigns, so ensuring that mail filters are well tuned and combined with DMARC records will cut down on malicious messages.**

## ANTIVIRUS

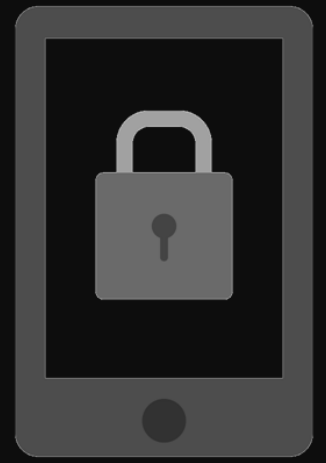
**Newer antivirus products include ransomware defense and analysis techniques that minimize the chances of an infection gaining a real foothold.**

## NETWORK SECURITY

**Outdated and unpatched systems, unnecessarily open ports, and untuned firewalls are all open holes attackers use to sneak into organizations and wreak havoc on a network.**

## BACKUPS

**Good, offline backups are the best failsafe for when things go wrong. Backups should also be taken regularly and tested for completeness.**



# LEADER'S RESPONSE


### Train Staff

Take advantage of training opportunities for your staff and yourself such as FedVTE's Elections IT Leader course, Cybrary for technical staff from FDOS, and Navigator trainings.

### Prepare for Disaster

Cyber incident response should be incorporated into disaster recovery planning and business continuity planning in order to ensure orderly response should the worst happen.

### Adopt a Framework

Tools like the FVRS MOA for Minimum Security Standards, NIST Cybersecurity Framework, and/or CIS Controls can help guide your plans, interactions with vendors, and back funding requests with requirements.

### Assess Gaps

Review your current posture compared to the framework(s) you choose to adopt and then create a plan on ways to address any issues. Work with your Cyber Navigator, CISA, or others if you would like assistance.

As an IT leader, you don't have to have a strong technical background to guide your staff through today's threat landscape. Focus on cyber hygiene, following a framework, and basic defense measures to prevent most attacks.

# SOE RESOURCES

You don’t have to face cyberthreats alone.

There are State and Federal resources available to assist you in securing your environment.

- Cyber Navigators
  - Navigator Training Program
  - Microsoft Teams Alerts
  - GAP Analysis\Assessments
  - Security Architecture
  - Tabletop Exercises
  - Incident Assistance
  - And More

- CISA Resiliency Review

https://us-cert.cisa.gov/resources/sltt

- Tabletop Exercises

- FedVTE

https://fedvte.usalearning.gov/

- Center for Internet Security’s EI-ISAC

https://www.cisecurity.org/ei-isac/

- Threat Intel

- System Security Guidelines

- ALBERT Monitoring


file edit folder tools info help
img_134.jpg
img_6856.jpg
img_1189.jp
img_6856.jpg
RANSOMWARE ATTACK
PAY TO UNLOCK YOUR FILES