HOW BAD COULD IT BE?

Lessons Learned from the Largest Coordinated Attack Against Local Government in US History

HOW DID I GET HERE?

I get asked a lot about how to get into cybersecurity and how to become a CISO and I usually give the consulting answer... " It depends"

There is no one path to becoming a CISO but here is a little about the path I took and how I ended up here with you today.


8:36 AM

THE STORY

IT ALWAYS HAPPENS ON A FRIDAY...

On Friday, August 16th, 2019, at 8:36 AM, the first call telling me there was yet another ransomware incident going on somewhere in the state came in.

But this one was not like the others.

This was the beginning of the largest coordinated attack of its kind in US history.

2017 WAS ACTION PACKED WITH ISSUES!

2017

Rising prevalence of ransomware attacks across the globe

2017

Lack of dedicated cybersecurity budgets and resources for state and local entities

2017

Insufficient incident response and recovery planning across the public sector (really all sectors)

2017

Growing threat of nation-state sponsored cyber threats targeting critical infrastructure

2017

"Somebody should do something"

2017

HB8 goes into effect on September 1

2017

Monday, September 11
Andy Gets a New Job

9:30 AM

4 Locals have reported being hit

Still no commonalities

Just a bad Friday

And the weekend isn't looking good...

BUILDING A COALITION FOR STATEWIDE INCIDENT RESPONSE PLANNING (OR WHEN PLANNING FOR ANY OTHER CONTINGENCY)

- **Convening Key Stakeholders**
  Bringing together representatives from state/federal agencies, to define and develop a state wide approach to address the growing specter of a massive scale cyber attack
- **Fostering Collaboration and Information Sharing**
  Everyone wants to know what's happening, but no one wants to share what is happening to them
- **Developing Incident Response Plan**
  Collaboratively crafting a comprehensive incident response plan to enable coordinated, effective, and timely actions during cyber incidents.
- **Securing Resources**
  Leverage existing emergency management processes and resource access mechanisms
- **Establishing Governance and Protocols**
  Defining the governance structure, roles, and protocols to ensure the effective and streamlined operation of the statewide incident response planning group.
- **Informed by Practice**
  Even as the SWIRP was being developed the OCISO team and I responded to about 100 ransomware incidents in the run up to 2019
- **Defining Escalation Criteria**
  Analyzing the scope and impact of cyber attacks targeting local government infrastructure and services across Texas and the country.

10:30 AM

10+ Locals have reported being hit

Regional nexus building

Public safety implicated...

A very bad Friday, the weekend is done for...

Eisenhower said that “plans are useless, but planning is indispensable,” while Mike Tyson said that “everyone has a plan until they get punched in the mouth.” Together, these sentiments paint the whole picture when it comes to incident response. Having and maintaining a robust incident response plan is valuable, but training and preparation are what makes responders able to pivot as the landscape changes, and stay standing as the hits keep coming.

-Andy

Cybersecurity Dive July 30, 2021

LESSONS LEARNED THROUGH PLANNING AND PRACTICE

Communication is Key

Effective incident response requires clear and constant communication between all stakeholders to ensure a timely and coordinated recovery, often to people and organization we would not have even thought to include up front. Seek out the people who will want or need to know in advance to prevent them from becoming detractors after the fact.

Its always the lawyers

Waiting until an incident occurs to involve lawyers is significantly slower than proactively including them in the planning process to ensure timely and effective response.

Incident Response and Recovery Planning

The ability to swiftly and effectively respond to and recover from the ransomware attack is critical, emphasizing the need for comprehensive incident response and recovery plans tailored to the unique challenges faced by local governments.

Fundamentals are not in place

The attack (and every successful ransomware attack) highlights the necessity of robust backup and data redundancy strategies to ensure the continuity of critical services and the ability to restore systems and data in the event of a successful ransomware attack. MFA, segmentation, end point protection, nothing can be taken for granted.

Third Parties Matter... A Lot

Third-party vendors and suppliers can introduce significant cyber risks, as they may have weaker security controls and present additional attack vectors for malicious actors to exploit.

10:45 AM

The escalation triggers have been met

Time to activate the plan

Bosses called the Governor to declare a disaster

I headed to the State Emergency Operation Center to take the Hot Seat

10:47 AM

Honey, it is going to be a long weekend

JACKSON COUNTY AND THURSDAY AUGUST 15TH

June 2019

Jackson County is completely taken out by the Ryuk Ransomware gang.

Judge Jill Sklar declares a Countywide Disaster

We had a plan

We had a team

She had the courage

Instead of turning right that morning I turned left and drove 2 hours to Edna TX.

Response and recovery times are good

We got the lawyers moving and even brought one with us

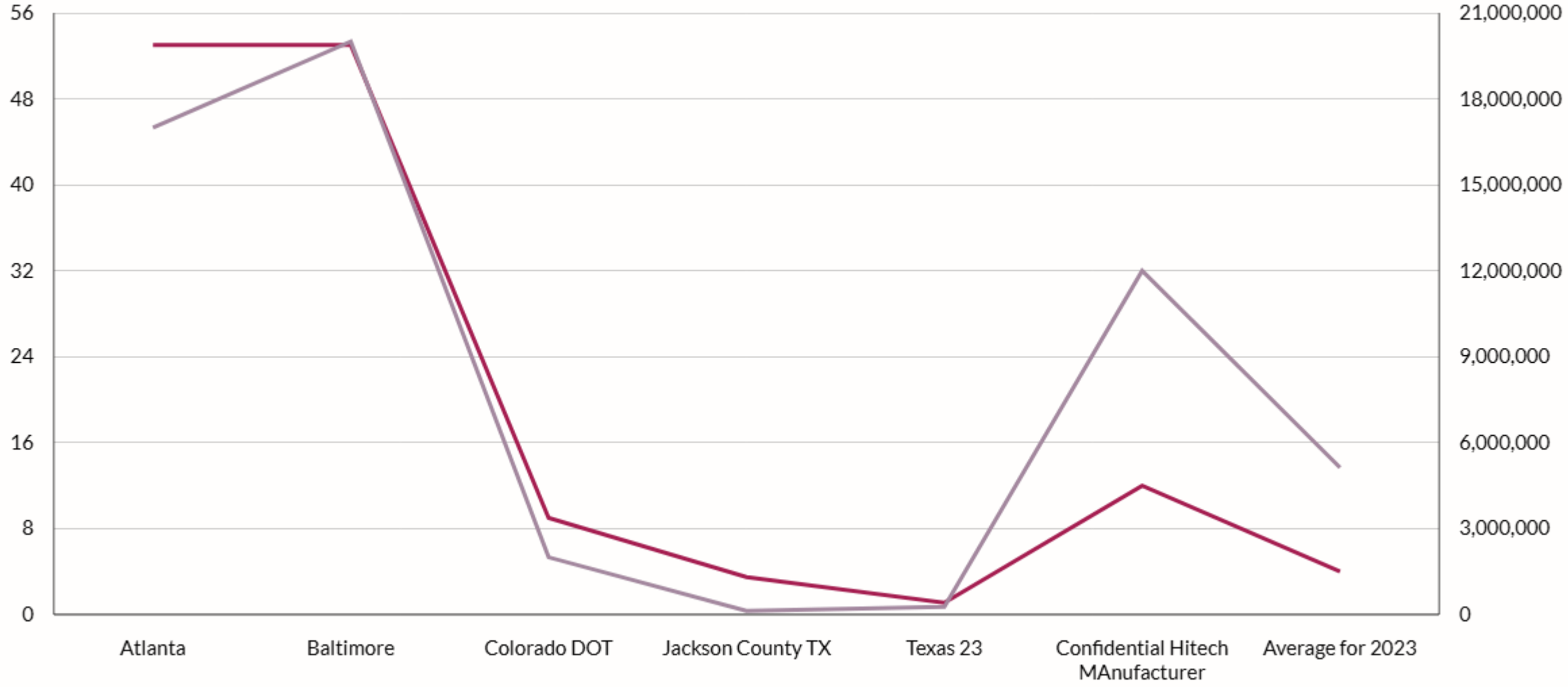
We got the teams engaged in hours not days

We were working on triage and restoration by lunch time and three weeks later the county was operational again.

Lessons Learned from the Attacks

The hotwash reviewing what worked and what needed improvement from the Jackson County response was held on the afternoon of August 15th, 2019…

Ransomware recovery times and cost examples



12:00 PM

The first call is scheduled

The plan is working

Everyone is staring at me

The rest of the week is a blur but the results speak for themselves

RICE COOKERS SHUT NYC SUBWAY
BOMB PRANK? TEST?
NYPD HUNTS FOR SUSPECT

DRUDGE REPORT

MOOCH UNLEASHED: TRUMP 'CRAZY'; 'PAPER TIGER' WHO WILL DROP OUT BY MARCH...

'Fattest President since William Howard Taft'...

FOXNEWS POLL: Losing to Biden, Warren, Sanders and Harris...

Energized and anxious: Liberals worry...

How Mayor Pete found God...

ISIS building caliphate 2.0...

ALIBABA co-founder buys NBA Nets; Highest price ever paid for US sports team....

DELTA passengers stranded on JFK runway for 8 hours...

Labor tensions flare at AMERICAN AIRLINES over hundreds of delays, canceled flights...

Workers flee Georgia poultry plant amid ICE rumors...

GREYHOUND riders asked for immigration papers at FL bus terminals...

Secret Service Locks Down Israeli Embassy After Threats...

Tlaib declines to visit West Bank...

Lawmaker at center of uproar...

WEEKEND: Hong Kong's Richest Man Warns Protesters and Beijing Against Violence...

CUSTOMS COMPUTERS SHUT DOWN
AIRPORTS SNARLED ACROSS USA

DRUDGE REPORT

MOOCH UNLEASHED: TRUMP 'CRAZY'; 'PAPER TIGER' WHO WILL DROP OUT BY MARCH...

'Fattest President since William Howard Taft'...

ISIS building caliphate 2.0...

ALIBABA co-founder buys NBA Nets; Highest price ever paid for US sports team....

Workers flee Georgia poultry plant amid ICE rumors...

GREYHOUND riders asked for immigration papers at FL bus terminals...

Secret Service Locks Down Israeli Embassy After Threats...

TEXAS UNDER RANSOMWARE ATTACK

20 LOCAL GOVTS HIT

DRUDGE REPORT

FACEBOOK pressured therapists to leak confidential employee info...

Warren Chips Away at Biden's Strength as One Who Beats Trump...

Energized and anxious: Liberals worry...

Signs of recession worry President ahead of 2020...

Held call with bank CEOs as stock market plunged...

BUCHANAN: Great tariff gamble...

Americans more in debt than ever...

Average owes $38,000...

Peter Fonda Dead at 79...

British Armed Forces in retention crisis...

ISIS building caliphate 2.0...

USA MOVES TO SEIZE IRAN OIL TANKER...

Kennedy Mulls Mass. Senate Run...

https://web.archive.org/web/20190817214218if_/https://www.drudgereport.com/

TEXAS UNDER RANSOMWARE ATTACK

20 LOCAL GOVTS HIT

DRUDGE REPORT

PIG HEART TRANSPLANTS HOPE...

CHINA LOOKING TO GENE EDIT ANIMALS...

Deepfake evidence so realistic 'innocent people will go to jail'...

Alaska's warmest month on record...

USA MOVES TO SEIZE IRAN TANKER...

Saudi Oil Plant Attacked by Drones...

Kennedy Mulls Mass. Senate Run...

https://web.archive.org/web/20190817224935if_/https://www.drudgereport.com/

TENSE IN PORTLAND

DRUDGE REPORT

The Daily Mail
The Drudge Report
Krebs on Security

Restore vs Recover

We restored operation to all 23 impacted entities in 8 days flat at a total cost to the taxpayers of just $274,000

To understand what that means, think like a firefighter or a first responder who needs to ensure life safety first.

KEY TAKEAWAYS WHEN PLANNING TO BE RESILIENT

- The plan is a starting point
- Contracts and Contacts
- Incident Response is Business Continuity Planning
- Funding and Resources
- Continuous Improvement is the Real Goal

Surprises and Pet Peeves

- No Such Thing as Superman
  - Everyone has to sleep and eat
- Life Still Happens
  - Wife texted at 6:35PM on the 16th that she had food poisoning
- Be Flexible and ask for help
  - We had outside help from unexpected places
- We were almost at the limit
  - If it ad been 40 the story might be very different
- Victim blaming is very real
  - These are evil people doing evil things and regardless of your level of preparedness, being attacked is still not your fault

Let’s finish the story:

Happy ending and incarceration

In November of 2021 two men were charged in connection with these attacks.
On Wednesday May 1st of 2024, one of them was sentenced to 13 years in a US Federal Prison

It is only a matter of time until the other(s) are too.

But what does the badguy look like?

- This young man literally ran a group known as Revil…
- He and his compatriots stole $700M and held thousands of companies, hospitals, governments and people hostage.
- But he may not look anything like what you expected.

Fundamentals

- MFA
- Segmentation
- Backups
- IR Plan
- Training

Thank you… Questions?

Andy Bennett
CTO, CISO, Apollo Information Systems
andy@apollo-is.com

See Speakers notes on this slide for resources