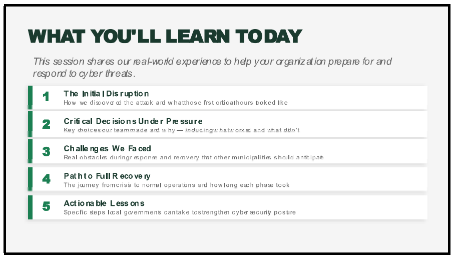
The information provided here is for informational and educational purposes and current as of the date of publication. The information is not a substitute for legal advice and does not necessarily reflect the opinion or policy position of the Municipal Association of South Carolina. Consult your attorney for advice concerning specific situations.

RANSOMWARE ATTACK

CITY OF ANDERSON

Lessons from the Front Lines
June 17-29, 2018



WHAT YOU'LL LEARN TODAY

This session shares our real-world experience to help your organization prepare for and respond to cyber threats.

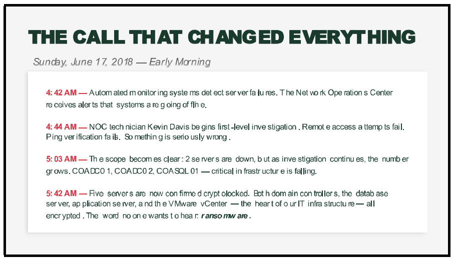
1 **The Initial Disruption**
How we discovered the attack and what those first critical hours looked like

2 **Critical Decisions Under Pressure**
Key choices our team made and why — including what worked and what didn't

3 **Challenges We Faced**
Real obstacles during response and recovery that other municipalities should anticipate

4 **Path to Full Recovery**
The journey from crisis to normal operations and how long each phase took

5 **Actionable Lessons**
Specific steps local governments can take to strengthen cyber security posture



THE CALL THAT CHANGED EVERYTHING

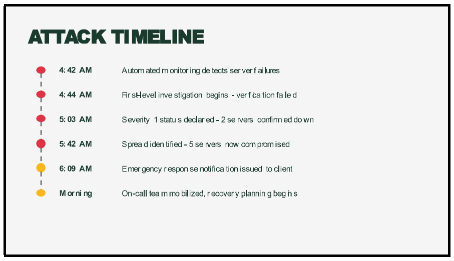
Sunday, June 17, 2018 — Early Morning

4:42 AM — Automated monitoring systems detect server failures. The Network Operations Center receives alerts that systems are going offline.

4:44 AM — NOC technician Kevin Davis begins first-level investigation. Remote access attempts fail. Ping verification fails. Something is seriously wrong.

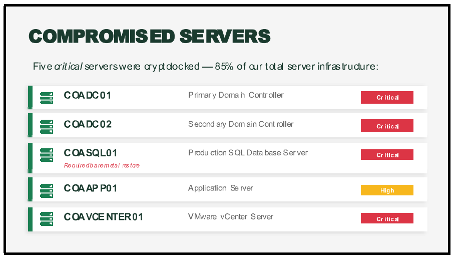
5:03 AM — The scope becomes clear: 2 servers are down, but as investigation continues, the number grows. COADC01, COADC02, COASQL01 — critical infrastructure is falling.

5:42 AM — Five servers are now confirmed cryptolocked. Both domain controllers, the database server, application server, and the VMware vCenter — the heart of our IT infrastructure — all encrypted. The word no one wants to hear: ***ransomware*.**



ATTACK TIMELINE

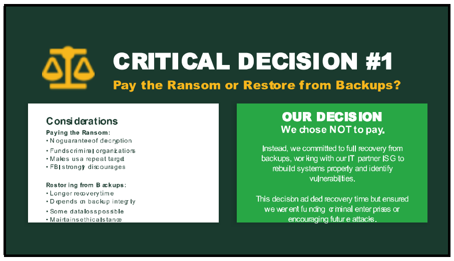
4:42 AM	Automated monitoring detects server failures
4:44 AM	First-level investigation begins - verification failed
5:03 AM	Severity 1 status declared - 2 servers confirmed down
5:42 AM	Spread identified - 5 servers now compromised
6:09 AM	Emergency response notification issued to client
Morning	On-call team mobilized, recovery planning begins



COMPROMISED SERVERS

Five *critical* servers were cryptolocked — 85% of our total server infrastructure:

COADC01	Primary Domain Controller	Critical
COADC02	Secondary Domain Controller	Critical
COASQL01 *Required bare metal restore*	Production SQL Database Server	Critical
COAAPP01	Application Server	High
COAVCENTER01	VMware vCenter Server	Critical



CRITICAL DECISION #1

Pay the Ransom or Restore from Backups?

Considerations

Paying the Ransom:
- No guarantee of decryption
- Funds criminal organizations
- Makes us a repeat target
- FBI strongly discourages

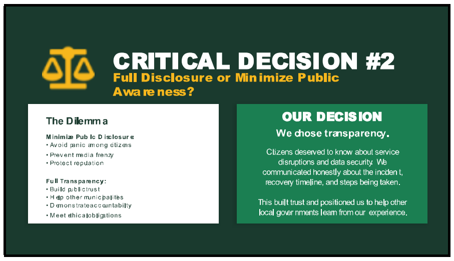
Restoring from Backups:
- Longer recovery time
- Depends on backup integrity
- Some data loss possible
- Maintains ethical stance

OUR DECISION

We chose NOT to pay.

Instead, we committed to full recovery from backups, working with our IT partner ISG to rebuild systems properly and identify vulnerabilities.

This decision added recovery time but ensured we weren't funding criminal enterprises or encouraging future attacks.



CRITICAL DECISION #2

Full Disclosure or Minimize Public Awareness?

The Dilemma

Minimize Public Disclosure
- Avoid panic among citizens
- Prevent media frenzy
- Protect reputation

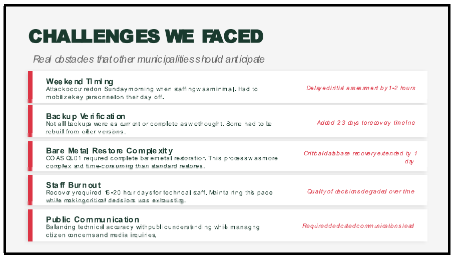
Full Transparency:
- Build public trust
- Help other municipalities
- Demonstrate accountability
- Meet ethical obligations

OUR DECISION

We chose transparency.

Citizens deserved to know about service disruptions and data security. We communicated honestly about the incident, recovery timeline, and steps being taken.

This built trust and positioned us to help other local governments learn from our experience.



CHALLENGES WE FACED

Real obstacles that other municipalities should anticipate

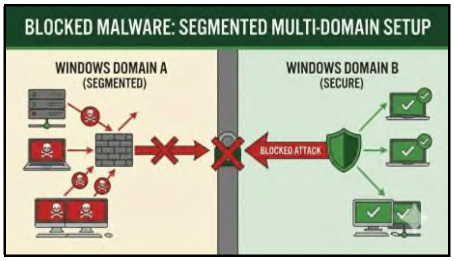
Weekend Timing
Attack occurred on Sunday morning when staffing was minimal. Had to mobilize key personnel on their day off.
Delayed initial assessment by 1-2 hours

Backup Verification
Not all backups were as current or complete as we thought. Some had to be rebuilt from older versions.
Added 2-3 days to recovery timeline

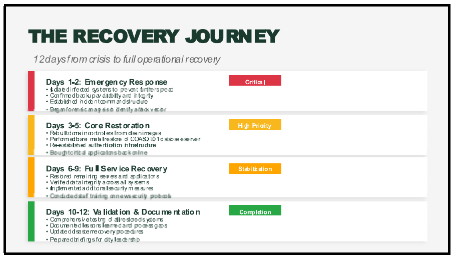
Bare Metal Restore Complexity
COASQL01 required complete bare metal restoration. This process was more complex and time-consuming than standard restores.
Critical database recovery extended by 1 day

Staff Burnout
Recovery required 16-20 hour days for technical staff. Maintaining this pace while making critical decisions was exhausting.
Quality of decisions degraded over time

Public Communication
Balancing technical accuracy with public understanding while managing citizen concerns and media inquiries.
Required dedicated communications lead



BLOCKED MALWARE: SEGMENTED MULTI-DOMAIN SETUP



THE RECOVERY JOURNEY

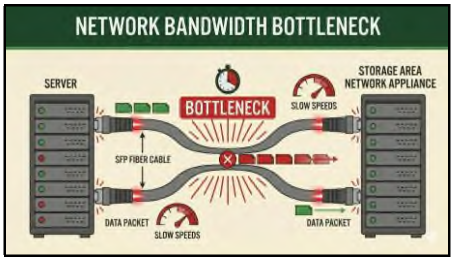
12 days from crisis to full operational recovery

Days 1-2: Emergency Response — Critical
- Isolated infected systems to prevent further spread
- Confirmed backup availability and integrity
- Established incident command structure
- Began forensic analysis to identify attack vector

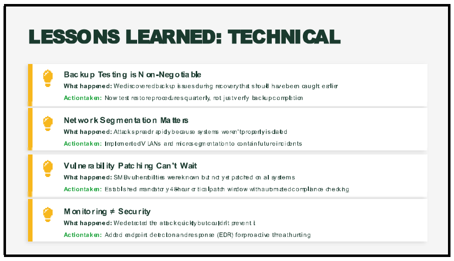
Days 3-5: Core Restoration — High Priority
- Rebuilt domain controllers from clean images
- Performed bare metal restore of COASQL01 database server
- Re-established authentication infrastructure
- Brought critical applications back online

Days 6-9: Full Service Recovery — Stabilization
- Restored remaining servers and applications
- Verified data integrity across all systems
- Implemented additional security measures
- Conducted staff training on new security protocols

Days 10-12: Validation & Documentation — Completion
- Comprehensive testing of all restored systems
- Documented lessons learned and process gaps
- Updated disaster recovery procedures
- Prepared briefings for city leadership



NETWORK BANDWIDTH BOTTLENECK



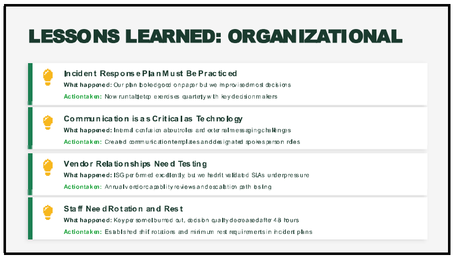
LESSONS LEARNED: TECHNICAL

Backup Testing is Non-Negotiable
What happened: We discovered backup issues during recovery that should have been caught earlier
Action taken: Now test restore procedures quarterly, not just verify backup completion

Network Segmentation Matters
What happened: Attack spread rapidly because systems weren't properly isolated
Action taken: Implemented VLANs and microsegmentation to contain future incidents

Vulnerability Patching Can't Wait
What happened: SMB vulnerabilities were known but not yet patched on all systems
Action taken: Established mandatory 48-hour critical patch window with automated compliance checking

Monitoring ≠ Security
What happened: We detected the attack quickly but couldn't prevent it
Action taken: Added endpoint detection and response (EDR) for proactive threat hunting



LESSONS LEARNED: ORGANIZATIONAL

Incident Response Plan Must Be Practiced
What happened: Our plan looked good on paper but we improvised most decisions
Action taken: Now run tabletop exercises quarterly with key decision makers

Communication is as Critical as Technology
What happened: Internal confusion about roles and external messaging challenges
Action taken: Created communication templates and designated spokesperson roles

Vendor Relationships Need Testing
What happened: ISG performed excellently, but we hadn't validated SLAs under pressure
Action taken: Annual vendor capability reviews and escalation path testing

Staff Need Rotation and Rest
What happened: Key personnel burned out, decision quality decreased after 48 hours
Action taken: Established shift rotations and minimum rest requirements in incident plans

Contained and eradicated in 48 hours.

WHAT YOU CAN DO

Actionable Steps to Strengthen Your Cybersecurity Posture

IMMEDIATE ACTIONS (0-30 DAYS)

Start here — these require minimal budget and can be done quickly

Test Your Backups — Critical
Don't just verify they complete — actually restore a server and confirm it works. Do this quarterly.

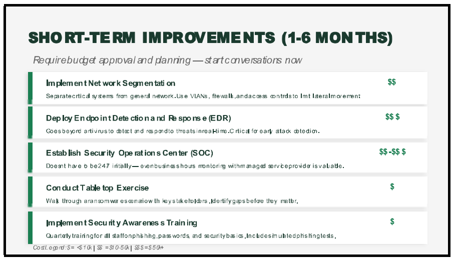
Review Patch Status — Critical
Identify all systems >30 days behind on security patches. Create a remediation plan with timelines.

Document Your Assets — High
Create an inventory of all servers, their roles, and interdependencies. You can't protect what you don't know about.

Verify Incident Contacts — Critical
Who do you call at 2AM on a Sunday? Make sure phone numbers are current and people answer.

Review Insurance Coverage — High
Cyber insurance can offset costs, but policies vary widely. Understand what's covered and excluded.

Enable MFA Everywhere — Critical
Multi-factor authentication on all administrative accounts and remote access. No exceptions.



SHORT-TERM IMPROVEMENTS (1-6 MONTHS)

Require budget approval and planning — start conversations now

Implement Network Segmentation $$
Separate critical systems from general network. Use VLANs, firewalls, and access controls to limit lateral movement.

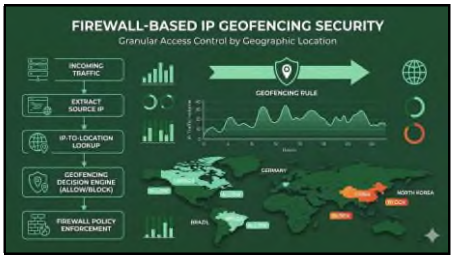
Deploy Endpoint Detection and Response (EDR) $$$
Goes beyond antivirus to detect and respond to threats in real-time. Critical for early attack detection.

Establish Security Operations Center (SOC) $$-$$$
Doesnt have to be 24/7 initially — even business hours monitoring with managed service provider is valuable.

Conduct Tabletop Exercise $
Walk through a ransomware scenario with key stakeholders. Identify gaps before they matter.

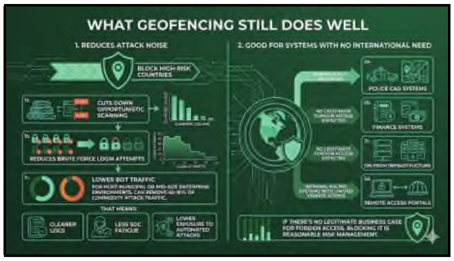
Implement Security Awareness Training $
Quarterly training for all staff on phishing, passwords, and security basics. Includes simulated phishing tests.

Cost Legend: $ = <$10k | $$ = $10-50k | $$$ = $50k+



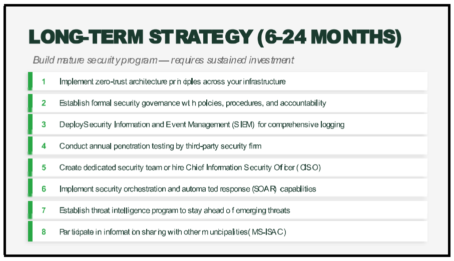
FIREWALL-BASED IP GEOFENCING SECURITY

Granular Access Control by Geographic Location



WHAT GEOFENCING STILL DOES WELL

1. REDUCES ATTACK NOISE
BLOCK HIGH-RISK COUNTRIES
CUTS DOWN OPPORTUNISTIC SCANNING
REDUCES BRUTE FORCE LOGIN ATTEMPTS
LOWER BOT TRAFFIC
FOR MOST MUNICIPAL OR MID-SIZE ENTERPRISE ENVIRONMENTS, CAN REMOVE 40-80% OF COMMODITY ATTACK TRAFFIC.
THAT MEANS:
CLEANER LOGS
LESS SOC FATIGUE
LOWER EXPOSURE TO AUTOMATED ATTACKS
2. GOOD FOR SYSTEMS WITH NO INTERNATIONAL NEED
NO LEGITIMATE FOREIGN ACCESS EXPECTED
NO LEGITIMATE FOREIGN ACCESS EXPECTED
POLICE CAD SYSTEMS
FINANCE SYSTEMS
ON-PREM INFRASTRUCTURE
REMOTE ACCESS PORTALS
IF THERE'S NO LEGITIMATE BUSINESS CASE FOR FOREIGN ACCESS, BLOCKING IT IS REASONABLE RISK MANAGEMENT.



LONG-TERM STRATEGY (6-24 MONTHS)

Build mature securityprogram — requires sustained investment

1 Implement zero-trust architecture pr in ciples across your infrastructure

2 Establish formal security governance wt h polcies, procedures, and accountability

3 DeploySecurity Information and Event Management (S IEM) for comprehensive logging

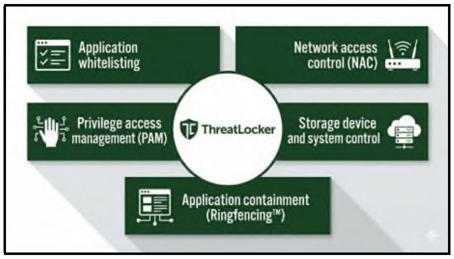
4 Conduct annual penetration testing by third-party security firm

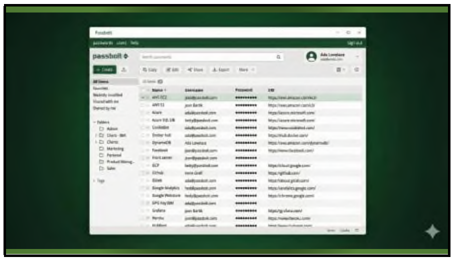
5 Create dedicated security team or hire Chief Information Security Of ficer (CISO)

6 Implement security orchestration and automa ted response (SOAR) capablities

7 Establish threat intelligence program to stay ahead o f emerging threats

8 Par ticipate in informat ion shar ing with other m unicipalities(MS-ISAC)


Application whitelisting
Network access control (NAC)
Privilege access management (PAM)
ThreatLocker
Storage device and system control
Application containment (Ringfencing™)



THE **REALITY CHECK**

You don't need to do everything.

Start with what makes sense for YOUR organization's size, budget, and risk profile.

The goal isn't perfect security — it's being prepared enough that when (not if) an incident occurs, you can respond effectively, recover quickly, and learn from the experience.

KEY TAKEAWAYS

WHEN, NOT IF

DECISIONS AHEAD

PRESSURE
PREPARED

RESTORE IS KEY

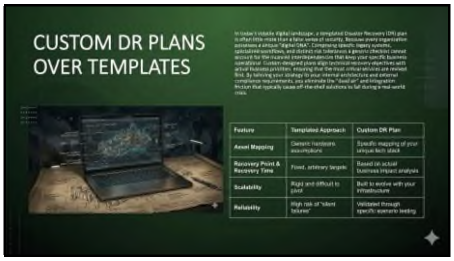
COMMUNICATE EFFECTIVELY

DON'T PAY

START SMALL

TODAY
TOMORROW
FUTURE

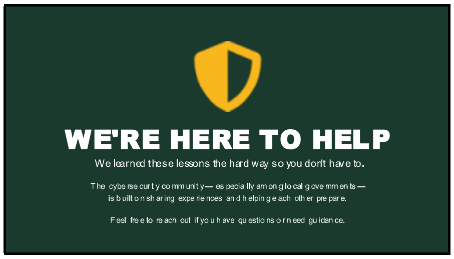
DISASTER IMMUNITY CONFIGURATOR
TAILORED INCIDENT RESPONSE
SYSTEM DATA BACKUP SCHEMA
PERSONALIZED, CLIENT-CENTRIC RESILIENCE PLAN
BESPOKE DR PLAN: INDIVIDUALLY CRAFTED
DISASTER TOLERANCE: MAXIMUM (CLIENT CONFIGURATION)
AFFECTED NODES: ISOLATED, SECURE
RESTORATION: TAILORED & RAPID (SYSTEM SPECIFIC)
VERIFICATION: CERTIFIED IMMUNITY LOG (CLIENT SIGNATURE)
DISASTER IMMUNITY CONFIGURATION
TAILORED RECOVERY INFRASTRUCTURE
BESPOKE



CUSTOM DR PLANS OVER TEMPLATES

In today's volatile digital landscape, a templated Disaster Recovery (DR) plan is often little more than a false sense of security. Because every organization possesses a unique "digital DNA", comprising specific legacy systems, specialized workflows, and distinct risk tolerances, a generic checklist cannot account for the nuanced interdependencies that keep your specific business operational. Custom-designed plans align technical recovery objectives with actual business priorities, ensuring that the most critical services are revived first. By tailoring your strategy to your internal architecture and external compliance requirements, you eliminate the "dead air" and integration friction that typically cause off-the-shelf solutions to fail during a real-world crisis.

Feature	Templated Approach	Custom DR Plan
Asset Mapping	Generic hardware assumptions	Specific mapping of your unique tech stack
Recovery Point & Recovery Time	Fixed, arbitrary targets	Based on actual business impact analysis
Scalability	Rigid and difficult to pivot	Built to evolve with your infrastructure
Reliability	High risk of "silent failures"	Validated through specific scenario testing



WE'RE HERE TO HELP

We learned these lessons the hard way so you don't have to.

The cybersecurity community—especially among local governments—is built on sharing experiences and helping each other prepare.

Feel free to reach out if you have questions or need guidance.